APLICACION DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE CONTROL EN LA ESTACIÓN TENAY DEL OLEODUCTO

HERNAN MAURICIO ROJAS PEÑA

Trabajo de grado presentado como requisito parcial para optar al título de Especialista En Seguridad Informática

Asesor: Martin Camilo Cancelado Ruiz

Neiva- Huila
Universidad Nacional abierta y a distancia
Ciencias básicas, tecnologías e ingeniería
2019

Nota de aceptación

_____

Presidente del jurado

_____

Jurado

_____

Jurado

_____

Neiva- Huila, 17 de Julio del 2019

Dedico este trabajo de grado en primera instancia a Dios, quien siempre me regalo su bendición, a mi bella familia mi esposa y mi hija que son el motor de mi vida y me impulsaron a alcanzar esta nueva meta, a mis padres que siempre me brindaron su apoyo de manera incondicional, a mis maestros asesores y directores de UNAD quienes me enseñaron el valor de perseverancia y entrega. A todos mil gracias.

AGRADECIMIENTOS

Al Ing. Martin Camilo cancelado Ruiz
Director de proyecto de grado

CONTENIDO

Lista de gráficos

Lista de tablas

1 TÍTULO DEL PROYECTO

APLICACION DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE CONTROL EN LA ESTACIÓN TENAY DEL OLEODUCTO.

2 INTRODUCCIÓN

El activo más importante que se posee en las organizaciones de hoy en día es la información, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena y en la implementación de técnicas que brinden la seguridad lógica. Estas barreras consisten en la aplicación de procedimientos que resguardan el acceso a los datos y sólo permitan acceder a ellos a las personas autorizadas para hacerlo.

Para lograr el aseguramiento se debe implementar un sistema de medidas de seguridad informática que incluya el establecimiento de las políticas y procedimientos que conforman una estrategia de cómo tratar los aspectos de seguridad. La base de este proceso radica en la realización de un análisis de riesgos que implica el examen de cada uno de ellos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir en la información de la compañía.

Con el ánimo de buscar buenas practicas que ayuden a mejorar y administrar de manera segura los sistemas de información se plantea la implementación de la metodología Magerit. En éste se proporciona una metodología para identificación, calificación y cuantificación del riesgo al que se ve expuesta la organización. Además, es el primer paso hacia la implementación de un sistema de gestión de seguridad informática ISO 27001.

La Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad. Estas cuestiones derivan en la existencia de una serie de normas y estándares, aceptadas como acreditaciones de la Seguridad de la Información, y cuya implementación aporta a la organización no sólo una certificación reconocida sino también como punto fundamental, una cultura y práctica de la seguridad que le aporta valores al negocio o servicio en muy diferentes aspectos, tales como: Mejora de la competitividad, mejora de la imagen corporativa, protección y continuidad del negocio, cumplimiento legal y reglamentario, optimización de recursos e inversión en tecnología, reducción de costes entre otros.

3 PLANTEAMIENTO DEL PROBLEMA

Actualmente, son muchas las empresas en Colombia que han actualizado sus sistemas de tratamiento de activos digitales, en procesos relacionados con el manejo de las tecnologías de la información y las comunicaciones (TICs). Con las herramientas que estos procesos le brindan para su actualización e innovación técnica y tecnológica, permite realizar las actividades diarias de manera eficiente optimizando recursos y tiempo. Este tipo de actividades han ido aumentando en la red de una manera rápida y crítica, ya que muchos de los procesos ejecutados no cuentan con una debida seguridad de la información, haciendo que sea más vulnerable ante cualquier amenaza o riesgo de hurto informático. Es por esto que deben existir técnicas que permitan asegurar más allá de la estructura física. La base de este proceso radica en la realización de un análisis de riesgos que implica el examen de cada uno de ellos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir en la información de la compañía. Este tipo de técnicas las podemos ubicar en la seguridad lógica, la cual consiste en la aplicación de barreras y procedimientos que protegen el ingreso a los datos y en su administración sólo permiten acceso al personal autorizado, al igual que con la implementación de políticas y procedimientos se pretende mantener la seguridad de la información.

La Estación Tenay del Oleoducto (OAM), se encentra ubicada al norte de la ciudad de Neiva en el departamento del Huila, es la estación de bombeo principal de uno de los oleoductos más importantes del país, se encarga de recolectar los crudos producidos por los campos petroleros del Huila y Tolima. Para llevara a cabo esta labor tan importante cuenta con un sistema de supervisión y adquisición de datos desde el cual puede operar de manera remota y controlada el transporte de hidrocarburos.

Pero este sistema tan importante para el país presenta graves problemas de seguridad en los sistemas informáticos ya que los datos almacenados no se encuentran protegidos y podríamos perder información de vital importancia para la operación. Sumado a esto la gran cantidad de puntos de acceso a la red sin control, aumenta la probabilidad de que cualquier persona tanto externa como interna que tenga acceso a uno de estos puntos de red podría tener acceso a la información del proceso que se encuentra almacenada en los servidores, lo que le permitiría cometer cualquier tipo de ataque al sistema y lo que sería peor podría generar una catástrofe ambiental por medio del sabotaje operacional.

Teniendo en cuenta que uno de los activos más importantes que tiene el OAM hoy en día, es la información y, por lo tanto, se debe implementar técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena y en la implementación de técnicas que blinden la seguridad lógica. Estas barreras consisten en la aplicación de controles y procedimientos que

resguarden el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

4 JUSTIFICACIÓN

En la actualidad las organizaciones tienen un alto flujo de información, flujos de servicios convergentes, flujo de activos y presupuestos en digital, así como una constante transferencia de información como el activo más preciado e importante de las empresas, pero este gran avance tecnológico trae consigo un gran problema de inseguridad informática que atenta contra uno de los activos más preciados de las compañías.

Por esto nace la necesidad de implementar una metodología que permita realizar una identificación, cuantificación del riesgo y que brinde las herramientas para proponer una serie de controles efectivos para evitar y/o mitigar la exposición ante ataques informáticos, y llevando el riesgo residual a niveles aceptables por la compañía. Los sistemas de información deben cumplir su objetivo, estar siempre disponibles para servir de apoyo a las diferentes actividades que realizan. No obstante, con la constante evolución de las computadoras, las redes sociales y de datos es fundamental saber que recursos necesitan seguridad en los sistemas de información y más aún cuando la información a proteger es el insumo primario para la operación de un oleoducto de más de 400 km de extensión, por esto es importante identificar las vulnerabilidades del sistema y plantear la o las soluciones más convenientes para mitigar la exposición a un ataque informático.

Teniendo como antesala las nuevas tendencias, informáticas y la desmaterialización de la información a partir de la eliminación de los papeles físicos como único soporte con valor probatorio, tradicionalmente reconocido, esta desmaterialización de los documentos llega a Colombia como una alternativa que no sólo se encuentra soportada por lo que exige la ley, sino que genera un entorno de confianza digital que está a la vanguardia de los requerimientos mundiales, los problemas y confusiones que se han presentado en temas de archivos y expedición de documentos físicos han demostrado que para las empresas es muy importante el costo y beneficio de digitalizar la información, ya que no sólo hace eficiente los procesos internos y externos, sino que asegura la perpetuidad de los mismos.

Mediante la implementación de la metodología Magerit La Estación Tenay del Oleoducto desea minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información del sistema de información que posee la estación.

Por lo tanto, el área encargada de la seguridad informática, mediante la implementación de una metodología de gestión del riesgo permitirá identificar, controlar y evitar eventos que comprometan el rendimiento de la organización.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Realizar un análisis de riesgos aplicando la metodología Magerit para los sistemas de control en la estación Tenay del Oleoducto

5.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento del estado actual de la empresa, de las metodologías de análisis y gestión de riesgos, controles informáticos de los sistemas de supervisión y control en la Estación Tenay del Oleoducto.
- Realizar análisis y gestión del riesgo a los que se ve expuesto los sistemas informáticos de supervisión y control en la Estación Tenay del Oleoducto, mediante la metodología Magerit.
- Proponer un diseño planificado de la solución incluido los costos y el ciclo de mejora continua, para los sistemas informático de supervisión y control en la Estación Tenay del Oleoducto.

6 MARCO CONCEPTUAL

6.1 SEGURIDAD DE LA INFORMACIÓN

Es toda actividad, que busca proteger todos los datos organizados y clasificados relevantes para una organización y o personas, ya sean información pública o privada, que busca evitar que la información sea filtrada y se vulnera su confidencialidad, sea modificada y afectada en su integridad y el no repudio.

6.1.1 Seguridad informática

"Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable".[1]

6.1.2 Mecanismos de seguridad

"Todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática. Se clasifican en: Preventivos: Actúan antes de que se produzcan ataques. Su misión es evitarlos. Detectores: Actúan cuando el ataque se ha producido y antes que cause daños en el sistema. Correctores: Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño".[2]

6.1.3 Seguridad pasiva

"Está construida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas podemos llamarlas de corrección." [3] (Aguilera López, Purificación, 2010).

6.1.4 Seguridad activa

"Los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo."[4] (Aguilera López, Purificación, 2010).

---

[1] Aguilera López, Purificación. Seguridad Informática, Citado por Galeano Villa, Jorge. Protocolo de políticas de seguridad informática para las universidades de Risaralda. [En línea]. Colombia: Universidad Católica de Pereira. 2013. p. 25. Disponible en https://docplayer.es/5605322-Protocolo-de-politicas-de-seguridad-informatica-para-las-universidades-de-risaralda-jorge-luis-galeano-villa-cristian-camilo-alzate-castaneda.html

[2] ibíd., p. 25.

[3] ibíd., p. 26.

[4] ibíd., p. 26.

6.1.5 Seguridad física

"Se utiliza para proteger el sistema informático utilizando barreras y mecanismos de control. Se emplea para proteger físicamente el sistema informático. Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales."[5]

6.1.6 Seguridad lógica

"Se encarga de asegurar la parte del software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos."[6]

6.1.7 Integridad de la información

Busca proteger los datos almacenados de daños, alteraciones y/o modificaciones de manera no autorizada por el custodio de la información. Estas alteraciones se presentan de ocasionalmente de manera intencional por personal externo o interno o de manera accidental en mayor medida por personal interno y/o administradores de sistemas.

6.1.8 Autenticidad

Son una serie de credenciales que autorizan o no el acceso a información confidencial, garantizando que el funcionario cuente con los permisos y autorizaciones definidas previamente por la compañía para poder hacer uso de los datos almacenados.

6.1.9 No Repudio

Es la manera de garantizar que el emisor de un mensaje sea la persona por medio de credenciales previamente parametrizadas y que el receptor este totalmente seguro que la persona que encabeza el mensaje sea la correcta, un ejemplo de esto sería el envió de un correo electrónico en donde se garantiza la plena identificación del emisor y receptor del mensaje.

6.1.10 Vulnerabilidad

Las vulnerabilidades de los sistemas informáticos son todas aquellas debilidades o puertas traseras que posibilitan que se materialice una pérdida de confidencialidad, integridad o no repudio de información.

---

[5] Aguilera López, Purificación. Seguridad Informática, Citado por Galeano Villa, Jorge. Protocolo de políticas de seguridad informática para las universidades de Risaralda. [En línea]. Colombia: Universidad Católica de Pereira. 2013. p. 26. Disponible en https://docplayer.es/5605322-Protocolo-de-politicas-de-seguridad-informatica-para-las-universidades-de-risaralda-jorge-luis-galeano-villa-cristian-camilo-alzate-castaneda.html

[6] ibíd., p. 26.

6.1.11 Amenaza

Es toda situación con un potencial de impacto suficientemente considerable para generar una pérdida de confidencialidad, integridad o no repudio de información. Estas amenazas pueden ser atribuidas a personas, equipos, desastres naturales, locativos, etc.

6.1.12 Riesgo

Es toda posibilidad de ocurrencia de potencia de daño a las personas, equipos, medio ambiente o imagen de la compañía. El riesgo normalmente es directamente proporcional con la vulnerabilidad, así que entre más grande sea esta mayor es el riesgo que se corre.

6.1.13 ISO 27000

"La serie de normas ISO/IEC 27000 se denomina requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI), proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa".[7]

- **ISO 27001:** "Que sustituye a la ISO 17799-1, abarca un conjunto de normas relacionadas con la seguridad informática. Se basa en la norma BS 7799-2 de British Estándar, otro organismo de normalización. Según esta norma, que es la principal de la serie, la seguridad de la información es la prevención de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento".[8]

- **ISO 27002**: "que se corresponde con la ISO 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendados relacionados con la seguridad".[9]

- **ISO 27003:** Contiene la guía que permite la implementación de la norma.
- **ISO 27004:** "Contiene los estándares en materia de seguridad para poder evaluar el sistema de gestión de la seguridad de la información".[10]

- **ISO 27005:** "Recoge el estándar para la gestión del riesgo de la seguridad".[11]

- **ISO 27006:** Dicta los requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO 27001.

---

[7] García, Alfonso, Hurtado, Cervigon, Seguridad Informática ED. 11: Informática y comunicaciones. 2011
[8] Ibíd., p. 19.
[9] Ibíd., p. 19.
[10] Ibíd., p. 19.
[11] Ibíd., p. 19.

- **ISO 27007:** "Es una guía de auditoría de un SGSI. Como un complemento a lo especificado en la ISO 19011".[12]

6.1.13.1 Análisis de Riesgos

El análisis de riesgos es una técnica o conjunto de técnicas, que busca estimar de manera cuantitativa o cualitativa la magnitud de los riesgos o vulnerabilidades a los que sean expuestos día a día las organizaciones, de esta manera poder realizar una efectiva selección de salvaguardas que ayuden a mitigar el impacto que este riesgo puedo causar a la organización teniendo en cuenta

6.1.13.2 Evaluación de Riesgos

Es una actividad que se debe implementar en las organizaciones y buscan eliminar los riesgos a los cuales se ve expuesta la organización, de no se r posible su eliminación, se definen una serie de controles que buscan minimizar el impacto hasta niveles aceptables para la compañía. Esta evaluación busca estimar de manera cuantitativa o cualitativa la magnitud de los riesgos.

6.2 Metodología para evaluación del riesgo

6.2.1 MAGERIT

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que busca gestionar de una forma sistemática los riesgos a los que se puede ver expuestos las diferentes organizaciones en temas relacionados a la seguridad informática. Esta metodología define objetivos claros trazables y alcanzables para las organizaciones y permite realizar un seguimiento exhaustivo del avance de los mismos.

6.2.1.1 Objetivos Magerit:

- "Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo."[13]
- "Ofrecer un método sistemático para analizar tales riesgos."[14]

---

[12] García, Alfonso, Hurtado, Cervigon, Seguridad Informática ED. 11: Informática y comunicaciones. 2011

[13] España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España, 8 p.

[14] Ibíd., p 8.

- “Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.”[15]
- “Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.”[16]
- “Ventajas de Magerit: Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.”[17]

6.2.1.2 Elementos Del Análisis De Riesgos

En la realización de un Análisis y Gestión de Riesgos según MAGERIT, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

- Activos: “Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información o dato”.[18]

- Amenazas: “Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza”.[19]

- Vulnerabilidades: “Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo”.[20]

- Impactos: “Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto”.[21]

- Riesgo: “Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia”.[22]

---

[15] España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España, 8 p.
[16] Ibíd., p 8.
[17] Ibíd., p 8.
[18] Ibíd., p 22
[19] Ibíd., p 27
[20] Ibíd., p 28
[21] Ibíd., p 29
[22] Ibíd., p 29

- Salvaguardas (Funciones, Servicios y Mecanismos): “Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas”.[23]

6.2.1.3 Implementación de la Metodología

La metodología Magerit, define un paso a paso para llevar cabo de manera satisfactoria la implementación del análisis de gestión de riesgos, los cuales se describen a continuación.

- Identificación de los activos más relevantes de la organización y descripción de los servicios e información que maneja.
- La valorización de los activos se realizará de manera cualitativa, teniendo en cuenta las siguientes dimensiones: su confidencialidad, su integridad, su disponibilidad, la autenticidad, la trazabilidad y el valor por interrupción del servicio.
    - Los activos son los elementos principales que una empresa posee para el tratamiento de la información. A la hora de iniciar un análisis de riesgo informático, se debe identificar los activos existentes en la organización y determinar el tipo.
- Definición de vulnerabilidades del sistema
    - Vulnerabilidad natural
    - Vulnerabilidad de hardware y software
    - Vulnerabilidad de los medios y/o dispositivos
    - Vulnerabilidad humana
- Definición de amenazas del sistema
    - De origen natural
    - Del entorno
    - Defectos de aplicaciones
    - Causadas por personas
    - Sistemas de comunicación
- Valoración del riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.
    - La probabilidad de ocurrencia la tomamos de las experiencias, históricos e informes emitidos por compañías que desarrollan la misma actividad económica.
    - El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.
    - zona 1 – riesgos muy probables y de muy alto impacto, representado por el color rojo

[23] España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España, 31 p.

- zona 2 –cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo, representado por el color naranja.
- zona 3 – riesgos improbables y de bajo impacto, representado con el color amarillo.
- zona 4 – riesgos improbables, pero de muy alto impacto, representado por el color verde.[24]

[24] España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España, 31 p.

7 MARCO TEÓRICO

7.1 DESCRIPCIÓN SISTEMA DE INFORMACIÓN PROPUESTO “SISTEMA DE SERVIDORES Y CLIENTES SISTEMA SCADA OLEODUCTO”

El Oleoducto, se encentra ubicado en el valle superior del magdalena y atraviesa los departamento del Huila, Tolima, caldas, Antioquia y Boyacá, cuenta con una estación de bombeo principal que se encuentra al norte de Neiva, la cual se encarga de recolectar los crudos producidos por los campos petroleros del Huila y Tolima y los transporta hacia la estación Vasconia y de ahí son transportados hacia Coveñas como crudo de exportación gracias a sus propiedades químicas. Para llevara a cabo esta labor tan importante cuenta con un sistema de supervisión y adquisición de datos desde el cual puede operar de manera controlada el transporte de hidrocarburos.

El sistema de control está compuesto por un enlace satelital, y una red de servidores interconectados entre sí mediante enlaces de fibra óptica desde donde se realiza toda la operación del oleoducto. En la actualidad la estación Tenay cuenta con dos redes de datos totalmente independientes, la primera es la Red Corporativa de la compañía desde la cual se puede tener acceso a la intranet e información clasificada de la misma; esta red cuenta con los protocolos de seguridad y administradores de red necesarios para asegurar la información. La segunda red es la Red Industrial que se encarga de recolectar la información de campo, almacenarla en los servidores, procesarla y presentarla de manera gráfica a los operadores del oleoducto.

La red industrial está compuesta por nueve puntos remotos que se comunican a través de enlaces satelitales, seis servidores, un computador de ingeniería desde donde se pueden hacer modificaciones a la base de datos y a las aplicaciones de visualización y procesamiento de datos, dos computadores de clientes y controladores que se encargan de recolectar la información de campo. Toda la red esta soportada por un sistema redundante de UPS de 30 KVA y un generador DIESEL de respaldo, el cual se enciende de manera inmediata tan pronto detecta problemas en el suministro eléctrico.

Ilustración 1. Arquitectura sistema SCADA

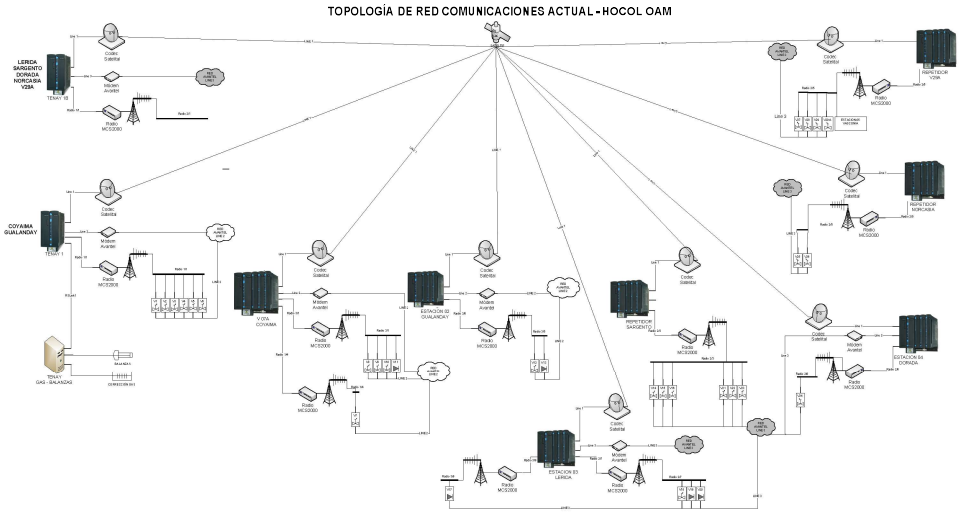

Ilustración 1. Arquitectura sistema SCADA

Fuente: Ingeniería de detalle sistema SCADA

Ilustración 2. Red sistema SCADA

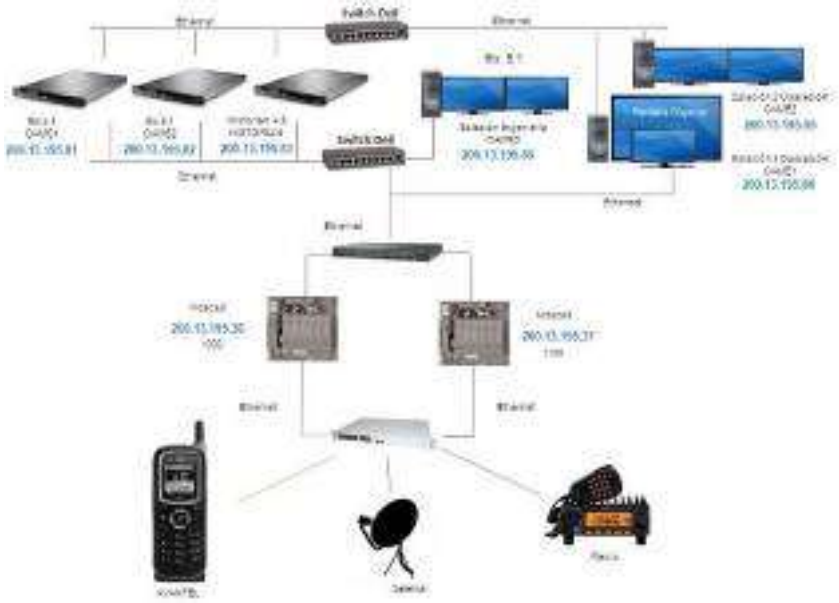

Ilustración 2. Red sistema SCADA

Fuente: Ingeniería de detalle sistema

Ilustración 3. Red sistema SCADA

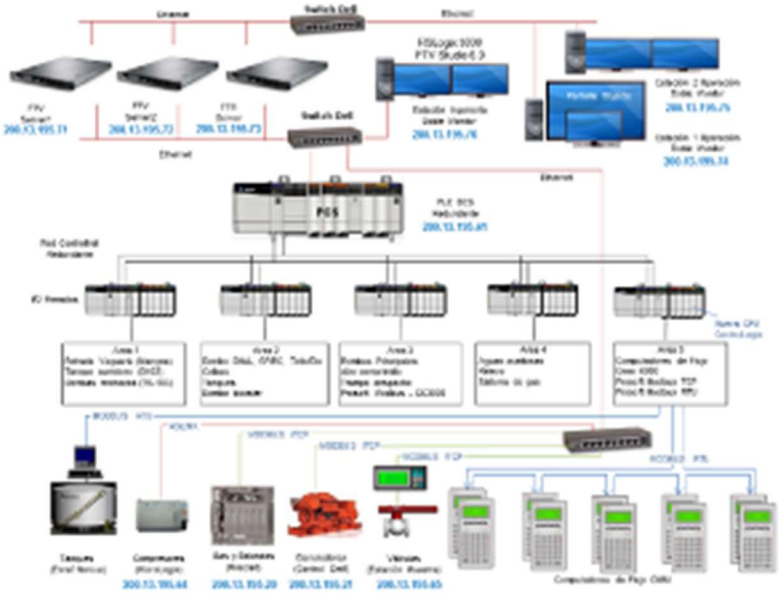

Ilustración 3. Red sistema SCADA

Fuente: Ingeniería de detalle sistema

7.2 SEGURIDAD DE LA INFORMACIÓN

Es toda actividad, que busca proteger todos los datos organizados y clasificados relevantes para una organización y o personas, ya sean información pública o privada, que busca evitar que la información sea filtrada y se vulnera su confidencialidad, sea modificada y afectada en su integridad y el no repudio. En la actualidad la información es considerada como un activo de altísimo valor, permite realizar al día millones de transacciones permitiendo acelerar el crecimiento de las economías, pero la mala manipulación de esta como por ejemplo una fuga de información podría hacer desplomar las acciones de compañía llevándola a la quiebra. Es por esto que se trabaja en proteger la información de cualquier ataque tanto interno como externo.

Hoy en día la seguridad de los sistemas informáticos atraen la mirada de los altos directivos de las compañías como de los entes gubernamentales quienes han tomado conciencia de los nuevos retos del siglo XXI, para esto se han comenzado a trabajar en políticas procedimientos y estándares nacionales e internacionales que buscan identificar y gestionar los riesgos informáticos.

La seguridad de la información define una serie de objetivos claros que ayudan a definir los caminos a seguir en el ámbito de seguridad informática los cuales se pueden resumir en:

- **Disponibilidad y accesibilidad de la información**: Este objetivo garantiza que la información este siempre disponible pero únicamente para el personal autorizado. Se busca que los datos se encuentren almacenados de manera segura tanto la parte lógica como la física, teniendo en cuenta que esta información es base fundamental para el desarrollo de las actividades de las compañías.

- **Integridad de la información:** Este objetivo garantiza que la información que se encuentra almacenada no sea alterada, modificada o borrada de manera parcial o total, garantiza siempre que los datos sean veraces evitando alteraciones por ataques informáticos o fallas humanas de los mismos colaboradores de las compañías. Entre estos tenemos:

    - **Integridad Datos**
    - **Integridad Sistemas**

- **Confidencialidad de la información:** este objetivo garantiza que la información solo será accedida por el personal autorizado, garantiza que los datos sean de uso privado durante al almacenamiento y envio de datos entre personal interno y externo de la compañía.

- **El no repudio de la información**: este objetivo garantiza la trazabilidad del uso y envió de información garantizando tanto el remitente como el receptor de los mensajes, así como las diferentes modificaciones que se realicen a los datos.

- **Confiabilidad de la información:** este objetivo se apalanca en los cuatro objetivos planteados con anterioridad, vela por que todos los lineamientos de seguridad estén aplicados y encaminados en pro de la seguridad además garantizar la información con la que se manejan las compañías.

Teniendo como antecedente que la seguridad informática busca mecanismos para proteger la información, esta se apoya en diferentes estándares como ISO 27001, que define los aspectos fundamentales que se listan a continuación:

- Determinar los objetivos, estrategias y políticas de Seguridad de la Información. [25]

- Determinar los requerimientos de Seguridad de la Información. [26]

- Identificar y analizar los riesgos de seguridad. [27]

- Especificar salvaguardas adecuadas teniendo en cuenta las amenazas, vulnerabilidades y riesgos identificados. [28]

- Supervisar la implementación y el funcionamiento de las salvaguardas especificadas. [29]

- Asegurar la concienciación de todo el personal en materia de Seguridad de la Información.[30]

- Detectar los posibles incidentes de seguridad y reaccionar ante ellos. [31]

En consecuencia y tomado a (Magerit Libro I - Método, 2012), "El enfoque global y de negocio de la Seguridad de la Información requiere de herramientas de gestión capaces de facilitar a los responsables la toma de decisiones. Entre estas herramientas de gestión, el análisis de riesgos permite identificar y valorar cuales son aquellas amenazas más relevantes para la seguridad de la información desde un punto de vista de negocio y la eficiencia de las salvaguardas establecidas para mitigar los riesgos asociados". [32]

7.3 ANÁLISIS Y EVALUACIÓN DEL RIESGO

El análisis de riesgo procesos sistemático que permite definir los distintos niveles de exposición potencial de riesgos con los que conviven las organizaciones, con esto se busca identificar todos estos factores de riesgo, con el animo de generar

[25] El portal de ISO 27001. ISO 27000.es, [En línea]. Colombia: Portal ISO 27001. 2014. p. 1. Disponible en http://www.iso27000.es/sgsi
[26] Ibíd., p 1.
[27] Ibíd., p 1
[28] Ibíd., p 1
[29] Ibíd., p 1
[30] Ibíd., p 1
[31] Ibíd., p 1
[32] España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España, 71 p.

procedimientos efectivos para el manejo de estos, buscando siempre eliminarlos y de no ser posible buscar mitigarlos hasta que el riesgo sea tolerable para la organización.

"El objetivo general del análisis de riesgos, es identificar sus causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para que se pueda tener información suficiente al respecto, optando así por un adecuado diseño e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados, en los diferentes puntos de análisis."[33]

"Otros objetivos específicos del proceso de análisis de riesgos son: analizar el tiempo, esfuerzo, recursos disponibles y necesarios para atacar los problemas; llevar a cabo un minucioso análisis de los riesgos y debilidades; identificar, definir y revisar los controles de seguridad; determinar si es necesario incrementar las medidas de seguridad; y la identificación de los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente."[34]

Los estándares más utilizados en la actualidad para la gestión del riesgo son:

- **NIST RMF:** Este estándar fue creado por el gobierno de los Estados Unidos de América EEUU, se trata de un sistema de identificación y evaluación de riesgos que se resume en seis pasos:

    - Calcificar la información
    - Seleccionar la información a evaluar
    - Implementar
    - Realizar la evaluación de riesgo
    - Autorización para implementación de salvaguardas
    - Control y seguimiento

- **OCTAVE:** Este estándar fue desarrollado por la universidad de Carnegie Mellon, y define un conjunto de métodos, técnicas y herramientas necesarios para desarrollar un análisis de riesgos

- **MAGERIT:** "Se trata de una metodología desarrollada por el Consejo Superior de Administración Electrónica dependiente del MAP, destinada en un principio a ayudar a los organismos de la administración pública española a conocer el riesgo a que estaban sometidos sus sistemas de información

[33] Bastidas, Henry. ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN [En línea]. Colombia: Universidad Nacional Abierta y A distancia UNAD. 2014. p. 43. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2668/5/76323713.pdf

[34] Ibíd., p 43.

MAGERIT describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos."[35]

[35] Bastidas, Henry. ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN [En línea]. Colombia: Universidad Nacional Abierta y A distancia UNAD. 2014. p. 45. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2668/5/76323713.pdf

8 MARCO METODOLÓGICO

8.1 ETAPA DE DIAGNÓSTICO

"En la etapa de diagnóstico se realiza un levantamiento de información de la organización con el fin de conocer la cultura organizacional; esto se realiza mediante las siguientes técnicas:" [36]

- "Lectura de la documentación existente (misión, visión, objetivos organizacionales, planeación estratégica, políticas, procesos, procedimientos, instructivos, manuales, normatividad entre otros). "[37]
- "Entrevistas a los líderes de proceso para conocer el clima organizacional y el estilo de liderazgo de la organización y de cada proceso. "[38]
- "Entrevistas a los líderes de proceso, mediante cuestionarios a los colaboradores de todos los niveles con el fin de conocer el grado de difusión del sistema de calidad y el nivel de empoderamiento de cada cargo. "[39]
- "Observación de procesos con el fin de hacer un diagnóstico organizacional del funcionamiento transversal de la estructura del mapa de procesos." [40]
- "Se continúa con el seguimiento a las actividades del cronograma."[41]
- "Se termina con un informe final de diagnóstico donde se determina con que documentación y procesos cuenta la organización y que hace falta para llegar a implementar las 3 normas que se desea, dando inicio a la siguiente etapa de planeación. "[42]

---

[36] Cortes, Diana. METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001 [En línea]. Colombia: Universidad EAN. junio 2012. p. 29. Disponible en https://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2&isAllowed=y

[37] Ibíd., p 29.

[38] Ibíd., p 29.

[39] Ibíd., p 29.

[40] Ibíd., p 29.

[41] Ibíd., p 29.

[42] Ibíd., p 29.

8.2 ETAPA DE PLANEACIÓN

"Para llevar a cabo esta etapa es necesaria la elaboración de un plan de trabajo detallado, donde se enumeren las actividades que se llevaran a cabo para poder implementar estas normas desde el punto de vista de la documentación. "[43]

- Creación de Grupos de trabajo
- Plan de trabajo: Al desarrollar el plan de trabajo para desarrollar esta metodología, es importante que:
    - Se identifiquen las tareas necesarias por realizar.
    - Se especifique un plazo para completar cada tarea.
    - Se indiquen claramente las relaciones de interdependencia entre las tareas establecidas.
    - Se designen personas o equipos específicos para llevar a cabo cada tarea.
    - Asignación de responsabilidades
    - Definición de recursos
    - Recursos humanos
    - Recursos físicos
    - Recursos financieros
    - Recursos técnicos
    - Capacitación del grupo de trabajo directivo y técnico

8.3 ETAPA DE DESARROLLO

"El paso a seguir es realizar el procesamiento y análisis de la información recolectada. Se deben definir que documentación es útil para el propósito de las certificaciones, eliminar los que estén duplicados y actualizar los que estén desactualizados o ayuden al cumplimiento de los requisitos de las normas."[44]

---

[43] Cortes, Diana. METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001 [En línea]. Colombia: Universidad EAN. junio 2012. p. 30. Disponible en https://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2&isAllowed=y

[44] Ibíd., p 35.

8.4 ETAPA DE PUESTA EN MARCHA DE LA IMPLEMENTACION

"Esta etapa se debe realizar la adecuación del sistema documental de la organización, contando con el visto bueno de la alta dirección y teniendo en cuenta las observaciones resultantes de la revisión gerencial."[45]

- Definición e implementación de política y objetivos de la seguridad informática
- Declaración de la aplicabilidad
- Plan de tratamiento de riesgos
- Marco legal y jurídico de la seguridad informática
- Definición de funciones y responsabilidades de seguridad.
- Política de seguridad para proveedores.

[45] Cortes, Diana. METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001 [En línea]. Colombia: Universidad EAN. junio 2012. p. 38. Disponible en https://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2&isAllowed=y

9 RESULTADOS Y DISCUSIÓN

9.1 PLAN DE CONTINUIDAD DEL NEGOCIO

9.1.1 Formulación De La Seguridad Informática En La Entidad

"Consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la entidad, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables."[46]

- **Que es una contingencia:** Definida como una eventualidad y/o fatalidad.

Teniendo como base esta definición se determina como situación para la activación del Plan de Contingencia una salida programada del sistema por más de media hora.

"El plan de contingencia cubrirá todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio alternativo y para lograrlo se deben revisar las operaciones cotidianas. Esto incluye cubrir los siguientes tópicos: hardware, software, documentación, talento humano y soporte logístico. "[47]

El establecimiento del plan de contingencia se inicia por la identificación de los procesos críticos de la entidad o aquellos que se tienen que ejecutar SIEMPRE.

La puesta en marcha de los planes a seguir es responsabilidad de cada coordinador de área y de los usuarios del sistema, además de todas las personas que de alguna forma ayudan a que el sistema cumpla con los requerimientos para el que fue diseñado, manteniendo sobre todo la integridad y confidencialidad de la información.

La vigencia de este plan está sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la empresa

---

[46] Tamayo, Jhnny. plan de contingencia informático [En línea]. Colombia: Universidad Nacional de Colombia Sede Manizales. 2003. p. 5. Disponible en http://bdigital.unal.edu.co/57872/1/plandecontingenciasinformatico.pdf

[47] Ibíd., p 7.

La vigencia de este plan está sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la empresa

9.1.2 Alcance

El alcance de la actividad es implementación de un análisis de riesgos basado en la metodología Magerit para el Oleoducto (OAM). dedicada al transporte de hidrocarburos por tubería, teniendo como actividad principal el recibo y transporte de crudo, medición tanto cantidad como calidad y fiscalización del mismo.

Por tal razón, el Oleoducto (OAM), debe contar con un Plan de Continuidad del Negocio que le permita recuperarse de incidentes que amenacen la prestación del servicio; para lo cual el Responsable de Seguridad de la Información elaborara el plan de continuidad del negocio y el Responsable de Sistemas de la Información, elaborara el plan de recuperación de desastres en materia tecnológica.

9.1.3 Objetivos

- Restablecer en el menor tiempo posible las funciones definidas como criticas, con el fin de reducir el impacto de manera que la correcta recuperación de los sistemas y procesos quede garantizada y se conserven los objetivos misionales del Oleoducto (OAM)

- Evaluar los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.

- Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.

- Presentar recomendaciones que permitan disminuir la probabilidad de ocurrencia de una eventualidad e implementar las acciones preventivas resultantes de estas.

- Listar posibles fallas que se pueden presentar en el funcionamiento del hardware y el software que conforman la plataforma tecnológica.

9.1.4 Organización

Deberes primarios de la implementación de la continuidad del negocio o de contingencia son:

- Proteger a los empleados y activos de información hasta que las operaciones normales sean reanudadas
- Asegurar que existe una capacidad viable para responder a un incidente
- Gestionar todas las actividades de respuesta, reanudación, recuperación y restauración.
- Apoyar y comunicarse con los empleados, administradores de sistemas, seguridad y gerentes.
- Garantizar los requisitos normativos están satisfechos.
- Ejercer decisiones reanudación y gastos de recuperación.
- Simplificar la notificación de reinicio y recuperación de progreso entre el equipos y gestión de cada sistema.

9.1.5 PROCESOS Y SERVICIOS A PROTEGER

Software:

- FACTORYTALK VIEW ME
- FACTORYTALK VIEW HISTORIAN
- FACTORYTALK VIEW STUDIO
- SCADA IFIX
- SCADA IFIX HISTORIAN

Servicios:

- Intranet
- Antivirus
- Software y ejecutables.
- Bases de datos clientes
- Backup de la información.

Activos:

- Personal
- Hardware
- Energía eléctrica.

- Comunicaciones.

Ocurrencia de daños:

- Daños físicos en las instalaciones por desastres naturales o influencia humana.
- Recursos informáticos desaparecidos por cambio de claves o eliminación física y lógica
- Fuga de información y que pueda afectar a la empresa

Causas de daños

- Acceso no autorizado a la información.
- Desastres naturales (terremotos, incendios, inundaciones, fallas en los equipos por cambios energéticos.
- Problemas con el personal de confianza (enfermedades, accidentes, retiros voluntarios y forzados etc)
- Fallas en el hardware y estructura física (servidores, en la red, swiches, cableado de red, router, firewall etc)
- Robos de equipos y archivos
- Virus informático

Servicios de apoyo logístico

Es importante aclarar que el presente documento tiende a contener únicamente el impacto por falla en la prestación del servicio de SISTEMAS DE COMPUTO.

Sin embargo la entidad debe tener contempladas las contingencias del Apoyo Logístico y tareas preventivas como son:

- Fluido eléctrico: Red regulada (UPS), Red Normal, Sistema de puesta a Tierra, Planta Eléctrica Principal y Alterna, Stocks de combustibles, Proceso manual de puesta en funcionamiento de estos dispositivos, prioridad para restablecer el servicio.

- Ambiente físico: Inundaciones, caídas de muros, Mantenimiento de infraestructura, Rutinas de Chequeo, rutas de evacuación, prioridad para restablecer el servicio.

- Iluminación: Planos eléctricos, mantenimiento, sistema de iluminación alterno, stocks, Proceso manual de puesta en funcionamiento de estos dispositivos

- Servicio de Agua: Tuberías, Motobombas, mantenimiento, Proceso manual de puesta en funcionamiento de estos dispositivos

- Aire Acondicionado: Ductos, desagües, mantenimiento

- Extintores: Tipo de Extintor de acuerdo a la ubicación dentro de la Empresa y el propósito para el cual debe ser utilizado.

- Señalización: Rutas de evacuación, ubicación departamentos y áreas críticas.

- Sistemas de Acceso: Proceso manual de desactivación de puertas y operación de botones anti pánico.

9.2 IDENTIFICACIÓN DE VULNERABILIDADES DEL SISTEMA

En la organización pueden presentarse muchos tipos de vulnerabilidades, a continuación, relaciono algunas de las más relevantes:

- **Ambiental/físicas:** La estación principal del oleoducto se encuentra expuesta a múltiples riesgos como lo son altas temperaturas, altas presiones y excesiva exposición a polvo generado por trabajos adyacentes a la sala de servidores y de clientes operadores. Riesgo a incendio debido a la cercanía con el centro de control de motores en donde se encuentran circuitos eléctricos de media y baja tensión.

- **Vulnerabilidades de hardware:** Por falta de programa de actualización de equipos y por falencias en el almacenamiento de los mismos.

- **Vulnerabilidades de software:** Por falta de actualizaciones de los equipos, ya que los servidores después de ser instalados y puestos en funcionamiento no se suelen volver a actualizar, por otra parte, las estaciones de trabajo se actualizan en desarrollo de aplicaciones y modificaciones en el HMI, pero el antivirus no es actualizado debido a que estas en ocasiones desactivan servicios de la aplicación y genera indisponibilidad del sistema.

- **Vulnerabilidades de medio de almacenaje:** No se cuenta con un lugar apropiado para almacenar de manera segura las copias de seguridad y los backup del sistema. Además, los usuarios finales pueden acceder a con medios magnéticos como discos duros portátiles y memorias USB a las estaciones de trabajo lo cual podría facilitar el robo de información y podrían afectar de manera intencional la disponibilidad del sistema y la integridad de la información almacenada.

- **Vulnerabilidad humana:** los operadores acceden las 24 horas del día los 7 días de la semana al sistema, por lo tanto, no tenemos control todo el día de las actividades adicionales que podrían desarrollar a lo largo de la jornada, el sistema se ve expuesto a posibles sabotajes, robo de información, y en ocasiones se ha detectado que utilizan las pantallas gigantes para ver películas y/ series de televisión.

- **Vulnerabilidades Socio-Educativa:** muchos de los operadores del sistema no cuentan con conocimiento profundo en sistemas y se limitan al uso básico del sistema, esto se debe a la falta de capacitación en seguridad informática y en el uso de los recursos informáticos, lo que generaría conciencia sobre el buen uso del sistema y el seguimiento en los procedimientos operacionales que se tienen.

9.2.1 Matriz de vulnerabilidades del sistema

Tabla 1. Matriz de vulnerabilidades

Ítem	**Vulnerabilidad ambiental / físicas**
1	Los equipos servidores del sistema SCADA están expuestos a polvo, debido a los trabajos que se realizan cerca de la sala de servidores.
2	Las áreas adyacentes presentas altas temperaturas debido al proceso petroquímico que se lleva a cabo dentro de las instalaciones
3	En las áreas adyacentes se encuentran tuberías con hidrocarburos a altas presiones debido al proceso petroquímico que se lleva a cabo dentro de las instalaciones
4	Cerca al centro de operaciones esta en centro de control de motores en donde se encuentran circuitos eléctricos de baja y media tensión, lo que podría generar un incendio en las estaciones de trabajo.
	Vulnerabilidad de hardware
5	No se cuenta con plan de actualizaciones de equipos.
6	No se controla el accedo de personal no autorizado
	Vulnerabilidades de software
7	No se mantienen los equipos actualizados

8	La clave de acceso al sistema es trivial y se encuentra escrita en un lugar visible a los visitantes.
9	El antivirus no se actualiza.
10	No se tiene configurado el firewall en los servidores
	Vulnerabilidades de medio de almacenaje
11	No se cuenta con un lugar apropiado para almacenar de manera segura las copias de seguridad y los backup del sistema.
12	Los puertos USB de las estaciones de trabajo están al alcance de los usuarios finales.
	Vulnerabilidad Humana
13	Los operadores y usuarios finales del sistema no tienen bases fuertes en el uso de sistemas informáticos
14	Los operadores y usuarios finales no tienen competencias técnicas en seguridad informática
15	El sistema en ocasiones está al alcance de personal ajeno a la operación.
16	El sistema está expuesto al posible robo de información.
17	El sistema está expuesto a posibles sabotaje sobre el sistema
	Vulnerabilidades Socio-Educativa
18	Falta de capacitación al personal que interactúa con el sistema
19	Falta de capacitación al personal que administra la red

Fuente: El Autor

9.2.2 Riesgos y amenazas

En todas las organizaciones y más en las que manejan grandes cantidades de datos e información, existen muchos riesgos, y el más alto puede repercutir en la pérdida del activo más importante, la información.

Podemos definir el riesgo como: la posibilidad de que ocurra algún evento negativo para las personas y/o empresas. Ya que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como

su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada.

> Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.[48]

RIESGO = AMENAZA x VULNERABILIDAD

9.2.3 Valoración matriz de riesgos por impacto y probabilidad

Escala Probabilidad

Alta: **A**
Media: **M**
Baja: **B**

Escala Impacto

Catastrófico: **C**
Moderado: **M**
Leve: **L**

Tabla 2. Valoración Matriz de riesgos

Riesgo / Valoración		Probabilidad			Impacto		
		A	M	B	L	M	C
R1	Daño de equipos informáticos (servidores y estaciones de trabajo) por exposición a polvo.			x			x
R2	Daño de equipos informáticos (servidores y estaciones de trabajo) por exposición a altas temperaturas.			x			x
R3	Daño de equipos informáticos (servidores y estaciones de trabajo) por explosión de tubería presurizada.			x			x

[48] Markus, Erb. Gestión de riesgo en la seguridad informática [En línea]. Suiza: amenazas y vulnerabilidades. 2003. p. 1. Disponible en https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

R4	Daño de equipos informáticos (estaciones de trabajo) por cortocircuito en celdas de potencia eléctrica.			x		x	
R5	No consecución de repuestos e equipos informáticos por obsolescencia.		x			x	
R6	Acceso de personal no autorizado a áreas restringidas	x			x		
R7	Falta de soporte por parte de los desarrolladores de software por obsolescencia.	x				x	
R8	Infección de virus por que se tiene el antivirus desactualizado.		x			x	
R9	Acceso no autorizado a los servicios y bese de datos de los servidores	x				x	
R10	Almacenamiento no seguro de copias de seguridad y backup del sistema	x				x	
R11	Los puertos USB no estas desactivas en las estaciones de trabajo	x			x		
R12	Robo de información confidencial	x					x
R13	Modificación de información confidencial	x					x
R14	Indisponibilidad del sistema informático por daños aleatorios	x					x
R15	Des configuración del sistema supervisorio por mal operación del sistema			x		x	
R16	Falta de competencias y aptitudes por parte de los usuarios finales		x		x		
R17	Acceso al sistema por personal no autorizado		x			x	
R18	Falla en las políticas de seguridad implementadas			X	x		
R19	Sabotaje externo			x		x	

Fuente: El Autor

9.2.4 Matiz de clasificación de riesgos

Tabla 3. Matriz de clasificación

	Leve	Moderado	Catastrófico
Alto	R6,R11	R7,R9,R10	R12,R13,R14
Medio	R16	R5,R8,R17	
Bajo	R18	R4,R15,R19	R1, R2, R3

Fuente: El Autor

9.3 DECLARACIÓN DE APLICABILIDAD

Tabla 4. Declaración de aplicabilidad

OBJETIVOS DE CONTROL	DOMINIOS	DESCRIPCIÓN - CONTROL	APLICABLE	JUSTIFICACIÓN	RAZÓN DE SELECCIÓN
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN					
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes interesadas	SI	Teniendo en cuenta, el core del negocio de la empresa, donde se maneja información altamente sensible a nivel de aplicaciones SACADA, y todo lo que puede implicar que dicha información caiga en manos fraudulentas, se requieren definir las políticas para la Seguridad de la Información aterrizadas a la realidad de la empresa, de acuerdo a los hallazgos realizados en el análisis de riesgos y a los demás controles que sean necesarios, donde se dejen claros los responsables de la aplicación.	Requerimientos del Negocio / Mejores Prácticas

				Igualmente para que esta sea efectiva se debe socializar con los empleados de la empresa y medir el grado de adherencia a las mismas.	
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Las políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	SI	Debido a la constante evolución de los sistemas informáticos, y de los diferentes mecanismos utilizados para la administración de la información se debe mantener en constante revisión las políticas establecidas de acuerdo a los métodos utilizados, para que vayan en el mismo sentido y haya un control efectivo de la Seguridad de la información.	Requerimientos del Negocio / Mejores Prácticas
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Se deben definir los responsables, y responsabilidades de acuerdo a la planeación estratégica, y definición del grupo implementador y auditor para la	Requerimientos del Negocio / Mejores Prácticas

Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.				respectiva implementación del SGSI	
	A 6.1.2 SEPARACIÓN DE DEBERES	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	SI	Se deben dejar muy bien delimitados los procesos, procedimientos y responsables de cada uno de ellos.	Resultado Análisis de riesgos
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	Se debe mantener contactos apropiados con las autoridades pertinentes.	SI	Se debe actuar bajo la normatividad vigente, y tener definido cuales son las autoridades responsables a las cuales se deben acudir en caso de requerirlo.	Requerimientos del Negocio / Mejores Prácticas
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	SI	Implementar directorio seguro, en el cual, podamos tener acceso a las últimas actualizaciones en materia de seguridad de la información y compartir información inherente al control del riesgo y a la	Requerimientos del Negocio / Mejores Prácticas

				minimización de las amenazas de seguridad	
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.	SI	Teniendo en cuenta la naturaleza de la empresa se debe prestar mayor atención a este control, ya que el core del negocio está enfocado al desarrollo de proyectos, con un alto contenido de confidencialidad debido a las plataformas que implementa.	Requerimientos del Negocio / Mejores Prácticas
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	Se deben adoptar una política unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	Se implementa política, la cual restringe y prohíbe la conexión de dispositivos móviles y equipos de personal externo a la red inalámbrica de la organización	Requerimientos del Negocio / Mejores Prácticas
	A 6.2.2 TELETRABAJO	Se deben implementar una política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o	NO	No se implementa debido a que la organización tiene un control sobre sus empleados y la información que se maneja, debido al alto grado de confidencialidad con que se debe manejar, por lo tanto se requiere la	Requerimientos del Negocio / Mejores Prácticas

		almacenada en los lugares en los que se realiza teletrabajo		presencia física del trabajador en un sitio específico de trabajo.	
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS					
A 7.1 ANTES DE ASUMIR EL EMPLEO Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran	A 7.1.1 SELECCIÓN	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	SI	Para el desarrollo de las actividades de Consultoría e Interventoría la organización requiere contratar personal, los cuales tienen acceso a la información de la compañía, por tanto es importante implementar controles basándose en los reglamentos, la ética y las leyes pertinentes, que aseguren un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información.	Requerimientos del Negocio / Mejores Prácticas
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	Los acuerdos contractuales con empleados y contratistas deben establecer sus	SI	Se deben dejar muy bien definido en la contratación, cual es el papel de cada uno de los actores, su	Requerimientos del Negocio / Mejores Prácticas

		responsabilidades y las de la organización en cuanto a seguridad de la información.		responsabilidad, y definir los acuerdos de confidencialidad entre empresa y empleado.	
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	SI	El personal contratado debe actuar bajo los estatutos de la empresa, y debe cumplir con cada uno de los procesos, procedimientos y políticas definidos bajo la implementación de los sistemas de gestión de las organizaciones.	Requerimientos del Negocio / Mejores Prácticas
Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones	SI	Se debe implementar plan de Inducción, actualización y capacitación de manera periódica en la organización con el fin de brindar la información oportuna de los cambios o modificaciones realizadas, a cada uno de los actores de los	Requerimientos del Negocio / Mejores Prácticas

		regulares sobre las políticas y procedimientos pertinentes para su cargo.		procesos, los cuales van encaminados al uso de las mejores prácticas en cuanto a Seguridad de la Información se refiere.	
	A.7.2.3 PROCESO DISCIPLINARIO	Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	Implementar comité disciplinario el cual se encargara de velar por el correcto actuar de los miembros de la empresa, y en caso de incumplir o actuar de manera errónea tomar los correctivos necesarios para evitar que estos actos se repitan, estos bajo la luz de la normatividad vigente.	Resultado Análisis de riesgos
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben redefinir, comunicar al empleado o contratista y se	SI	Implementar políticas de control de la información y de roles de seguridad, sobre cada uno de los empleados que tienen acceso a la información sensible de la organización, y suscribir los acuerdos de confidencialidad, con el empleado o contratista, con el fin de velar por la confidencialidad e	Resultado Análisis de riesgos

		deben hacer cumplir.		integridad de la información.	
A.8 GESTION DE ACTIVOS					
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A 8.1.1 INVENTARIO DE ACTIVOS	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	Se tienen definidas las hojas de vida y el inventario de activos, de cada uno de los componentes que hacen parte de la infraestructura tecnológica de la organización (Servidores, Switch, Dispositivos de seguridad, UPS, entre otros)	Requerimientos del Negocio / Mejores Prácticas
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	Los activos mantenidos en el inventario deben ser propios.	SI	Se tiene definido el proceso, y se cuenta con la herramienta tecnológica para la entrega, auditoria, devolución y control de cada uno de los activos entregados al empleado para el desarrollo de sus actividades diarias	Requerimientos del Negocio / Mejores Prácticas

	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	Se tienen definidas las políticas de uso, de cada uno de los dispositivos de computo, de red y demás pertenecientes a la infraestructura tecnológica, el cual define que esta o no permitido durante el desarrollo de las labores diarias.	Requerimientos del Negocio / Mejores Prácticas
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	Se tiene definido el proceso, y se cuenta con la herramienta tecnológica para la entrega, auditoria, devolución y control de cada uno de los activos entregados al empleado para el desarrollo de sus actividades diarias.	Requerimientos del Negocio / Mejores Prácticas
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN Asegurar que la organización recibe un	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	Se cuenta con un inventario de información, donde se encuentra discriminado el responsable, las fuentes de alimentación de las mismas, y los órganos encargados de la auditoría y control de	Resultado Análisis de riesgos

nivel apropiado de protección de acuerdo con su importancia para la organización.				cambios sobre la información; igualmente de acuerdo a su importancia hay un mayor grado de custodia y protección de la misma	
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se tiene estructurado el proceso que indica, cuál debe ser el rotulamiento de la información y cual debe ser la cadena de custodia correspondiente.	Requerimientos del Negocio / Mejores Prácticas
	A 8.2.3 MANEJO DE ACTIVOS	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Cada área responsable de información tiene acceso restringido solamente a la información requerida y generada en su actuar diario, por lo tanto esta es solo accesible por el personal a cargo de la misma.	Requerimientos del Negocio / Mejores Prácticas

A 8.3 MANEJO DE MEDIOS Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	Se tiene estructurado el procedimiento con las políticas de acceso a la información y la copia de la misma en medios extraíbles, con lo que se pretende limitar el acceso o copia indiscriminada de la misma por personal ajeno, a la misma.	Requerimientos del Negocio / Mejores Prácticas
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	SI	Se implementa procedimiento que estipula los periodos de tiempo de almacenamiento y custodia de la información, así como la disposición final que se le debe dar a cada uno de los mismos en los casos que esta cumpla con los periodos establecidos para su almacenaje.	Requerimientos del Negocio / Mejores Prácticas
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o	SI	Se tiene definido quienes son los responsables de la custodia de la información, y se tienen implementadas medidas para el control de acceso	Resultado Análisis de riesgos

		corrupción durante el transporte.		a la información confidencial.	
A.9 CONTROL DE ACCESO					
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	Estas medidas se tienen definidas en la política de seguridad de la información, basado en la asignación de perfiles y roles	Resultado Análisis de riesgos
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	Estos accesos son controlados por el administrador del sistema el cual por medio de la definición de los roles en el dominio corporativo controla el acceso a los recursos de la red.	Resultado Análisis de riesgos
A 9.2 GESTIÓN DE	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	SI	El procedimiento de asignación de perfiles, tiene definido la ruta de acceso al sistema donde cada responsable de área define de acuerdo a un formato establecido cuales son los roles que se deben asignar a cada	Resultado Análisis de riesgos

ACCESO DE USUARIOS Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	SI	uno de los empleados, dentro de la organización para controlar el acceso y seguridad de la información, al igual que describe el procedimiento a seguir para la cancelación de perfiles al retirarse de la institución, teniendo como punto de control la firma del paz y salvo del área responsable de la asignación de perfiles, con lo cual lo que se busca es eliminar todos aquellos permisos que se habían entregado al momento de la vinculación. Dentro del proceso de verificación y auditoria se tiene definido una revisión periódica de los logs de transacciones, con el fin de verificar que se estén cumpliendo los accesos a la información determinada solo por	
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI		
	A 9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	SI		
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	SI		

	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	parte de los responsables de la misma.	
A 9.3 RESPONSABILIDADES DE LOS USUARIOS Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	Cada acceso de usuario se hace por medio de las credenciales de acceso definidas en el procedimiento de asignación de perfiles y roles.	Resultado Análisis de riesgos
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la	SI	Estos controles están definidos en la política de seguridad y el procedimiento de asignación de perfiles y roles, el cual define el grado de acceso a los sistemas de información.	Resultado Análisis de riesgos

		política de control de acceso.			
Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	SI	El acceso a los sistemas de información desde sedes remotas por parte del personal autorizado, se realizan a través de VPN, donde se cuentan con unas credenciales asignadas al responsable de dicho acceso controlando así el acceso indiscrimado.	Resultado Análisis de riesgos
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	SI	Se tiene definido el control de contraseñas donde se tienen establecidos los parámetros mínimos de seguridad en la creación de las mismas, y la periodicidad de la actualización de las mismas.	Resultado Análisis de riesgos
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los	SI	Se tiene restringido la instalación de software y acceso al panel de configuración de los equipos, por parte de los empleados diferentes al área encargada de soporte de sistemas, de	Resultado Análisis de riesgos

		controles de las aplicaciones.		esta manera se limita el uso indebido de los equipos.	
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	Se debe restringir el acceso a códigos fuente de programas.	SI	Este se tiene definido de acuerdo a la clasificación de la información, y al control de acceso a la misma solo por parte del personal responsable del tratamiento de esta.	Resultado Análisis de riesgos
A. 10 CRIPTOGRAFIA					
A 10.1 CONTROLES CRIPTOGRAFICOS Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	SI	Teniendo en cuenta el core del negocio de la empresa, se deben implementar los controles criptográficos acordes a los diferentes proyectos desarrollados al interior de la empresa, esto con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información accesada a través de estos medios.	Resultado Análisis de riesgos
	A 10.1.2 GESTIÓN DE LLAVES	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas,	SI	Se debe implementar procedimientos que defina los tiempos vigencia de los controles definidos por la empresa al igual que la periodicidad con que se	Resultado Análisis de riesgos

		durante todo su ciclo de vida.		deben revisar y actualizar los mismos, acorde a la evolución de los mismos.	
A. 11 SEGURIDAD FISICA Y DEL ENTORNO					
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	El área de procesamiento central, racks de servidores y switches se encuentra delimitado por un área de acceso restringido, y al cual solo tienen acceso el personal encargado del área, o terceros bajo la supervisión de los responsables de la custodia del mismo.	Resultado Análisis de riesgos
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI	Para el acceso al área se tiene por medio de una llave especial, la cual se encuentra bajo custodia del personal responsable de dicha área y se lleva registro manual del acceso al área y en caso de requerirse el acceso de un tercero esta se realiza bajo supervisión del personal a cargo.	Resultado Análisis de riesgos
	A 11.1.3 SEGURIDAD DE OFICINAS,	Se debe diseñar y aplicar seguridad física a oficinas,	SI	El acceso a los equipos donde se procesa información se encuentra	Resultado Análisis de riesgos

Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	RECINTOS E INSTALACIONES	salones e instalaciones.		delimitada mediante oficinas cerradas donde solo tienen acceso el personal que allí labora, por medio del uso de tarjeta inteligente al área en general y uso de llaves a cada oficina.	
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	Se cuenta con protección eléctrica, sensores contra incendios, dispositivos extintores para la mitigación del fuego en caso que se requiera, pero igualmente se deben implementar las medidas necesarias en caso de inundaciones y otras que no se tienen controladas.	Resultado Análisis de riesgos
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI		Resultado Análisis de riesgos
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de	NO	El acceso y salida a la empresa solo puede realizarse a través de la única entrada que se tiene establecida y se tienen implementados controles de seguridad para impedir el libre acceso por parte de personal ajeno a las	Resultado Análisis de riesgos

		información para evitar el acceso no autorizado.		instalaciones de la empresa.	
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	SI	Se tienen definidas las políticas de seguridad que indica que debe hacerse en caso de un retiro temporal del sitio del trabajo y la protección de acceso a los sistemas por medio de las credenciales locales a nivel de equipo y de aplicativo.	Resultado Análisis de riesgos
	A 11.2.2 SERVICIOS DE SUMINSITRO	Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	SI	Se cuenta con protección eléctrica a través de la red regulada y la planta eléctrica, las cuales brindan el respaldo necesario para darle continuidad al negocio.	Resultado Análisis de riesgos
	A 11.2.3 SEGURIDAD EN EL CABLEADO	El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	SI	Se tienen racks bien estructurados en gabinetes y cuartos protegidos contra el libre acceso por parte del personal ajeno.	Resultado Análisis de riesgos

Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A 11.2.4 MANTENIMIENTO DE EQUIPOS	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Se tiene contratado personal a cargo del soporte preventivo y correctivo de los equipos pertenecientes a la red informática.	Resultado Análisis de riesgos
	A 11.2.5 RETIRO DE ACTIVOS	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	Se tiene definido el formato para el retiro de equipos de la empresa, donde se autoriza por las áreas encargadas de la custodia de los activos y se definen responsables y tiempos de devolución.	Resultado Análisis de riesgos
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios	SI	El acceso a los sistemas informáticos desde el exterior se hace mediante VPN, credenciales de acceso a la máquina, y se tienen contratadas las pólizas de respaldo ante eventualidades.	Requerimientos del Negocio / Mejores Prácticas
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento	SI	Se debe implementar procedimiento dentro del proceso de control de inventarios que defina, la rutina que se debe llevar	Requerimientos del Negocio / Mejores Prácticas

		para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.		a cabo antes de dar de baja a los activos que se encuentran fuera de su vida útil.	
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	SI	Se tienen definidas las políticas de seguridad que indica que debe hacerse en caso de un retiro temporal del sitio del trabajo y la protección de acceso a los sistemas por medio de las credenciales locales a nivel de equipo y de aplicativo.	Resultado Análisis de riesgos
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de	SI	Implementar procedimiento para tener bajo custodia la información física que no se esté utilizando, y la información magnética bien clasificada y almacenada en las respectivas carpetas de	Resultado Análisis de riesgos

		procesamiento de información.		acceso solo por la persona responsable de la misma.	
A.12 SEGURIDAD DE LAS OPERACIONES					
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	Se tienen definidos los procedimientos de acuerdo al proceso de sistema de gestión de seguridad de la información que se está implantando en la empresa y a las políticas de seguridad definidas.	Requerimientos del Negocio / Mejores Prácticas
	A 12.1.2 GESTIÓN DE CAMBIOS	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	Implementar políticas estables que garanticen la baja rotación de personal, y garanticen la estabilidad del sistema de gestión en general.	Requerimientos del Negocio / Mejores Prácticas
	A 12.1.3 GESTIÓN DE CAPACIDAD	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de	SI	Nombrar comité encargado de la planeación estratégica, que asegure los recursos necesarios para la sostenibilidad del sistema	Requerimientos del Negocio / Mejores Prácticas

		capacidad futura, para asegurar el desempeño requerido del sistema.		de gestión y la estabilidad de la empresa, siempre haciendo un uso adecuado de los recursos.	
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	SI	Delimitar cada uno de los departamentos específicos de la empresa, donde cada uno solo sea accesible por el personal a cargo del mismo.	Requerimientos del Negocio / Mejores Prácticas
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	Se tienen implementados dispositivos de seguridad perimetral, software a nivel local (antiviurs, antimalware, entre otros); y se hace socialización constante del buen uso de los recursos y de las técnicas usadas en la actualidad para vulnerar los sistemas.	Resultado Análisis de riesgos
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	Se deben hacer copias de respaldo de la información, software e imágenes	SI	Se tiene definido procedimiento de control de copias de seguridad donde se establecen los	Resultado Análisis de riesgos

Objetivo. Proteger contra la pérdida de datos.		de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.		recursos a los que se les hace copia, periodicidad, responsable y custodia de la misma.	
A 12.4 REGISTRO Y SEGUIMIENTO Objetivo. Registrar eventos y generar evidencia	A12.4.1 REGISTRO DE EVENTOS	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	SI	Se lleva un control de los registros de transacciones realizados por cada uno de los usuarios, a los cuales solo tiene acceso el administrador de la red, y la trazabilidad y auditoria de los mismos son revisados periódicamente por el coordinador del área de tecnología.	Resultado Análisis de riesgos
	A12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI		Resultado Análisis de riesgos
	A12.4.3 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	SI		Resultado Análisis de riesgos

	A12.4.4 SINCRONIZACIÓN DE RELOJES	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	Se tiene sincronizado el horario general de los diferentes dispositivos con el servidor del dominio, el cual es accesado solamente por el administrador de la red.	Resultado Análisis de riesgos
A 12.5 CONTROL DE SOFTWARE OPERACIONAL Objetivo. Asegurarse de la integridad de los sistemas operacionales	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	Se tiene restringido la instalación de software y acceso al panel de configuración de los equipos, por parte de los empleados diferentes al área encargada de soporte de sistemas, de esta manera se limita el uso indebido de los equipos.	Requerimientos del Negocio / Mejores Prácticas
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se	SI	Se tiene definido el análisis de riesgos de la empresa y la periodicidad de evaluación y seguimiento del mismo, con el fin de garantizar el tratamiento de los diferentes hallazgos	Resultado Análisis de riesgos

		usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.		encontrados al interior de la empresa.	
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	SI	Se tiene restringido la instalación de software y acceso al panel de configuración de los equipos, por parte de los empleados diferentes al área encargada de soporte de sistemas, de esta manera se limita el uso indebido de los equipos.	Requerimientos del Negocio / Mejores Prácticas
A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los	SI	Se tiene establecido el plan de mantenimiento de los sistemas informáticos de una manera periódica con el fin de realizar el respectivo afinamiento y garantizar el correcto funcionamiento del mismo.	Requerimientos del Negocio / Mejores Prácticas

		procesos del negocio.			
A. 13 SEGURIDAD DE LAS COMUNICACIONES					
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A 13.1.1 CONTROLES DE REDES	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	Se deben implementar las políticas de configuración de redes y restricción de acceso a la misma, por parte de personal externo o dispositivos ajenos a la empresa.	Resultado Análisis de riesgos
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	Se tienen suscritos contratos de confidencialidad con los proveedores de los servicios de red locales que prestan un servicio a la empresa.	Resultado Análisis de riesgos
	A 13.1.3 SEPARACIÓN EN LAS REDES	Los grupos de servicios de información, usuarios y sistemas de información se	SI	Se deben definir los segmentos de red de acuerdo al área y procesos realizados al interior de la empresa,	Requerimientos del Negocio / Mejores Prácticas

		deben separar en las redes.		con el fin de dar un mayor grado de seguridad al procesamiento de la información.	
A 13.2 TRANSFERENCIA DE INFORMACIÓN Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	SI	Se debe implementar las políticas y procedimientos dentro del sistema de gestión de la empresa para garantizar la integridad y confidencialidad de la información que sea compartida al interior de la empresa o por medio de correos electrónicos, limitando esto a que dicha actividad se realice por medio de los correos institucionales los cuales son administrados por la empresa y eliminando el riesgo que esta quede en cada uno de los correos personales de los empleados, y en la medida de lo posible hacer uso de las diferentes técnicas criptográficas o medios seguros para la transmisión de datos.	Requerimientos del Negocio / Mejores Prácticas
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI		Resultado Análisis de riesgos
	A 13.2.3 MENSAJERIA ELECTRÓNICA	Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	SI		Resultado Análisis de riesgos

	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	Se deben dejar muy bien definidos estos acuerdos de confidencialidad en los diferentes tipos de convenios y contratos suscritos por la empresa.	Requerimiento Legal
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	Los desarrollos realizados al interior de la empresa deben estructurarse basado en los avances en materia de seguridad informática, con el fin de desarrollar sistemas de información seguros, garantizando la actualización constante de los mismos, buscando siempre que estos cumplan con los pilares fundamentales de la seguridad de la información como lo son la disponibilidad, integridad y	Requerimientos del Negocio / Mejores Prácticas
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe	SI		Requerimientos del Negocio / Mejores Prácticas

prestan servicios sobre redes públicas.		proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		confidencialidad de la información	
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	SI		Requerimientos del Negocio / Mejores Prácticas
	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	Se deben establecer y aplicar reglas para el desarrollo de software y de	SI	Se tiene definida la ruta de navegación, para el desarrollo de sistemas de	Requerimientos del Negocio / Mejores Prácticas

A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE		sistemas a los desarrollos dentro de la organización.		información al interior de la empresa	
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante uso de procedimientos formales de control de cambio.	SI	Los cambios realizados al sistema en general se realiza de acuerdo a los requerimientos de los clientes y después del respectivo análisis de la viabilidad legal y técnica.	Requerimientos del Negocio / Mejores Prácticas
Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	Se tiene establecido el procedimiento que define como se deben realizar las baterías de pruebas, y cuales son los pasos a seguir para la verificación y documentación de las mismas.	Requerimientos del Negocio / Mejores Prácticas
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios,	SI	Los cambios realizados al sistema en general se realiza de acuerdo a los requerimientos de los clientes y después del	Requerimiento Legal

		y todos los cambios se deben controlar estrictamente.		respectivo análisis de la viabilidad legal y técnica.	
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguro, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	Los desarrollos realizados al interior de la empresa deben estructurarse basado en los avances en materia de seguridad informática, con el fin de desarrollar sistemas de información seguros, garantizando la actualización constante de los mismos, buscando siempre que estos cumplan con los pilares fundamentales de la seguridad de la información como lo son la disponibilidad, integridad y confidencialidad de la información	Requerimientos del Negocio / Mejores Prácticas
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI		Requerimientos del Negocio / Mejores Prácticas
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	La organización debe supervisar y hacer seguimiento	NO	La empresa al tener como core de negocio el desarrollo de	Requerimientos del Negocio / Mejores Prácticas

		de la actividad de desarrollo de sistemas contratados externamente.		aplicaciones, altamente sensibles se encarga de controlar y desarrollar cada una de las etapas en su totalidad al interior, para así evitar fugas de información.	
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	Se hacen uso de las técnicas y herramientas de pentesting, con el fin de identificar las posibles vulnerabilidades y de esta manera, tratar de contrarrestarlos.	Requerimientos del Negocio / Mejores Prácticas
	A 14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programa de prueba para aceptación y criterios de aceptación relacionados.	SI	Se tiene establecido el procedimiento que define como se deben realizar las baterías de pruebas, y cuáles son los pasos a seguir para la verificación, documentación y aprobación de las mismas.	Requerimientos del Negocio / Mejores Prácticas
A 14.3 DATOS DE PRUEBA Objetivo. Asegurar la protección de los datos usados para pruebas.	A 14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	Las pruebas se deben realizar por parte del personal encargado del área de pruebas, con los que se tienen suscritos acuerdos de confidencialidad, para	Obligaciones Contractuales

				garantizar el buen uso de la base de datos usada y la no divulgación de la misma.	
A.15 RELACIONES CON LOS PROVEEDORES					
A. 15.1 RELACIONES CON LOS PROVEEDORES	A 15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	SI	Se deben establecer unas políticas claras por parte de la empresa, en cuanto al tratamiento que se le deben dar a los contratos y convenios suscritos con los proveedores, encaminados a la protección de la información a la cual estos puedan tener acceso de acuerdo a la actividad contratada, al igual que se deben tener identificados los riesgos a los que se está expuestos, y las posibles medidas para contrarrestar dichos riesgos, y bajo ningún motivo se deben omitir suscribir ampliamente los acuerdos de confidencialidad y no divulgación de la posible	Obligaciones Contractuales
Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI	SI		Obligaciones Contractuales

		para la información de la organización.		información a la que pueda tener acceso el proveedor.	
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI		Obligaciones Contractuales
A 15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación de servicio en línea con los acuerdos con los proveedores.	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	La empresa debe gestionar constantemente para que los servicios contratados con terceros sean prestados por estos de buena calidad, y garantizando que los recursos y dispositivos entregados sean los adecuados para el desarrollo eficiente y seguro de la empresa, al igual que de la seguridad de la información.	Requerimientos del Negocio / Mejores Prácticas
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	Se deben gestionar los cambios en los suministro de servicios por parte de los proveedores, incluido el mantenimiento y la	SI		Obligaciones Contractuales

		mejora de las políticas, procedimientos y controles de seguridad de la información existente, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.			
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Se debe tener estructurado el plan de contingencia respectivo de acuerdo a las necesidades y a la realidad de la empresa, el cual les permita mediante su aplicación minimizar el impacto ante eventuales incidentes.	Requerimientos del Negocio / Mejores Prácticas
	A 16.1.2 REPORTE DE EVENTOS DE	Los eventos de seguridad de la información se deben informar a	SI	Se deben implementar y estructurar los canales de soporte y la plataforma de administración de	Requerimientos del Negocio / Mejores Prácticas

Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	SEGURIDAD DE LA INFORMACIÓN	través de los canales de gestión apropiados, tan pronto como sea posible.		eventos con el fin de categorizarlos y priorizarlos de tal manera que se le dé respuesta efectiva a cada uno de ellos de acuerdo a las variables de complejidad analizadas y al impacto que pueda generar al interior de la empresa, al igual que este servirá como insumo, para el respectivo análisis de indicadores y de esta manera poder tomar medidas, con respecto a las áreas afectadas y al mejoramiento de los mismos con el fin de contrarrestar futuros eventos que se puedan presentar por las causas ya identificadas, o las que se puedan desprender de aquí.	
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI		Requerimientos del Negocio / Mejores Prácticas
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI		Resultado Análisis de riesgos
	A 16.1.5 RESPUESTA A INCIDENTES DE	Se debe dar respuesta a los incidentes de	SI		Resultado Análisis de riesgos

	SEGUIRIDAD DE LA INFORMACIÓN	seguridad de la información de acuerdo procedimientos documentados.			
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI		Resultado Análisis de riesgos
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	La organización definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI		Resultado Análisis de riesgos
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO					
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la	SI	Se deben evaluar los procesos,	Requerimientos del Negocio / Mejores Prácticas

Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		procedimientos y políticas implementados bajo el marco del sistema de gestión que se viene implementando, y evaluar su impacto y efectividad al interior de la empresa, haciendo uso de herramientas de análisis y tratamiento de riesgos y de esta manera identificar las acciones de mejoras, las cuales se deben ver reflejadas en la actualización de los insumos del sistema de gestión que lo ameriten	
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI		Requerimientos del Negocio / Mejores Prácticas
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con	SI		Requerimientos del Negocio / Mejores Prácticas

		el fin de asegurar que son válidos y eficaces durante situaciones adversas.			
A 17.2 REDUNDANCIAS Objetivo. Asegurar la disponibilidad de instalaciones de procesamiento de información.	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	Se tienen implementada una infraestructura tecnológica que da cumplimiento a la continuidad del negocio, aplicando las técnicas de redundancia a nivel lógico como de hardware, soporte eléctrico, y a través de diferentes canales de internet que permiten levantar el servicio ante la ausencia de uno de los operadores	Requerimientos del Negocio / Mejores Prácticas
A. 18 CUMPLIMIENTO					
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y	SI	Se debe implementar un proceso de capacitación continuada de tal manera que cada uno de los integrantes de la empresa trabajen articulados de acuerdo a la normatividad vigente y permanezcan en constante actualización	Requerimiento Legal

Objetivo. Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		mantenerlos actualizados para cada sistema de información y para la organización.		ante los diferentes cambios presentados.	
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	Se tiene establecidos el control de instalación de software, limitando esta labor al personal encargado de soporte el cual solo puede realizar dichas instalaciones bajo los parámetros de licenciamiento adquirido	Requerimiento Legal
	A 18.1.3 PROTECCIÓN DE REGISTROS	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los	SI	Se tienen implementados procedimientos los cuales se documentaron regidos bajo la normatividad vigente e	Requerimiento Legal

		requisitos legislativos, de reglamentación, contractuales y de negocio.			
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	Los sistemas de información se encuentran desarrollados bajo la normatividad legal vigente, dada	Requerimiento Legal
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	Se adquieren y hacen uso de los controles criptográficos establecidos por la ley para el reporte de información oficial, los cuales garantizan la confidencialidad e integridad de la información presentada.	Requerimiento Legal
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN Objetivo. Asegurar que la seguridad de la	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es	SI		Requerimientos del Negocio / Mejores Prácticas

información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		Se tiene establecido una revisión periódica y una auditoria interna de los procesos implementados de acuerdo a la normatividad vigente, y a las actualizaciones que se realicen a la norma base de implementación.	
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Los directores deben revisar con regularidad el cumplimiento de procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI		Requerimientos del Negocio / Mejores Prácticas

	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI		Requerimientos del Negocio / Mejores Prácticas

Fuente: El Autor

9.4 PLAN DE TRATAMIENTO DE RIESGOS

9.4.1 Determinación de activos del Oleoducto OAM. y el riesgo existente.

Tabla 5. Determinación de activos del OAM

ELEMENTO EN RIESGO	RIESGO	FORTALEZA	DEBILIDAD	GN	FE	GI	ACCION
INSTALACIONES Y CUARTO TECNICO	Incendio, desastres naturales	Extintores situados estratégicamente cerca de las áreas más vulnerables y cargados. Respaldo, o backup. Vigilancia	- Capacitación al personal de elementos de seguridad Y DE primeros auxilios. - No existe banco de backup.	S	A	A	Correctiva: -Realizar capacitaciones al personal. -Almacenar información en lugares seguros y en la nube.
EQUIPOS Y ARCHIVOS	Robo	Retiro de equipos mediante formatos.	Falta personal de vigilancia. - Frecuentes pérdidas de accesorios.	G	A	M	Correctiva: - Responsabilizar a los empleados de los equipos a su cargo. Denunciar en caso de robo a mano armada.
EQUIPOS	Falla en los equipos Falla por fluido eléctrico.	Técnico especializado para mantenimiento. Se cuenta con UPS	-Falta de aseo en los equipos. -Hardware obsoleto. -Potencia de red.	G	A	M	-Manual de funciones para el técnico de mantenimiento. -Mantener contacto con

							proveedores para reponer las piezas o software.
EQUIPOS Y SOFTWARE	Manejo inadecuado del sistema	Personal experto en el área de sistemas	- Equivocaciones en el manejo del hardware y del software. -Personal inexperto. -Políticas claras y precisas	M	P	M	Capacitación al personal sobre manejo y políticas informáticas. Entregas de licencias, antivirus y claves confiables.
SOFTWARE	Virus Informático	Antivirus full. Acceso restringido al servidor, solamente el administrador	Renovaciones de licencias. Navegación por internet sin restricciones	S	C	A	- Restricciones en el manejo de internet. - Actualizaciones frecuentes. - Capacitaciones. -Crear correo institucional
SOFTWARE	Accesos no autorizados	Acceso al sistema de red mediante clave.	Falta comunicación acerca de retiro del personal.	G	AL	A	-Creación de correos - Reasignación de claves y permisos
HARDWARE Y SOFTWARE	Ausencia del personal de sistemas	Manual de procedimientos.	Solo una persona conoce las claves, el manejo de red.	G	AL	A	-Autorizar a una persona alterna que reemplace al administrador en caso de que falte.

			Inventarios actualizados.				-Revisar manual de procedimientos Levantamiento de diagrama lógico sobre las conexiones existentes.
SERVIDOR	Falla en el servidor	Personal capacitado en el área de sistemas	-Fallas corte de cable UTP -Fallas tarjeta de red. -Fallas IP asignado, punto de swicht, punto de Pacht Panel, punto de red	M	PR	B	Revisiones periódicas y reemplazo de piezas, Testeo de cable uTP, mantenimiento punto de red. Diagrama lógico de red.
EQUIPOS DE COMUNICACIÓN	Perdida del servicio de internet	Personal capacitado en el área de sistemas	Antenas, fibra óptica, redes, software	G	C	M	Revisión de componentes y reemplazo. Realizar pruebas de operatividad del servicio

Fuente: El Autor

La valorización de los activos se realizará de manera cualitativa, teniendo en cuenta las siguientes dimensiones:

- su confidencialidad
- su integridad
- su disponibilidad
- la autenticidad
- la trazabilidad
- el valor por interrupción del servicio.

Se realiza la identificación de los activos más relevantes de la organización y descripción de los servicios e información que maneja.

9.4.2 Identificación de activos

Tabla 6. Identificación de activos 1

Equipo	Información y servicios que maneja
Servidores web	Se encargan de ejecutar la capa de presentación e interactúan el resto de elementos del back-end.
Servidores de bases de datos	Se encarga de administrar los datos para el almacenamiento de datos de los diferentes estados de la aplicación y sus usuarios. Estos mismos servidores de bases de datos implementan otras bases de datos corporativas como son por ejemplo las del Sistema de Gestión de Proyectos.
Servidores de aplicación	Se utilizan como middleware entre la capa de presentación y el host. Estos elementos además sirven para simular todo el back-end que interacciona con la aplicación desarrollada, de modo que la organización no dispone de un host real.
Estaciones de trabajo	Se encargan de brindar las herramientas tecnológicas y accesos a los diferentes servidores de la organización, desde aquí se realizan los diferentes desarrollos de software.

Fuente: El Autor

Tabla 7. Identificación de activos 2

Equipo	Información y servicios que maneja
Redes de comunicación	Se encarga de proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores, entre los diferentes equipos informáticos de la compañía.
Las personas de la organización (Desarrolladores, usuarios operadores, clientes finales)	Se encarga de administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.
Instalaciones	Se encargan de salvaguardar la integridad de los activos de la compañía, al igual que protegerlos del acceso no autorizado de personal externo.
Aplicaciones	Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos dentro y fuera de la compañía, además permite comunicarse de manera asertiva con los servidores y clientes del sistema informático.
Suministro eléctrico	Se encarga de proveer alimentación eléctrica de buena calidad a todos los equipos electrónicos que conforman el sistema de información de la compañía.
Sistema de apantallamiento y puestas a tierra	Se encarga de proteger a las personas y de paso a los equipos informáticos de descargas eléctricas ocasionadas por descargas atmosféricas y corrientes

	parasitas de otros sistemas.

Para reestablecer el servicio en caso de una contingencia se requiere que estas cuentas con unas características mínimas las cuales se relacionan a continuación:

Tabla 8. Identificación de activos 3

Tipo de servicio	Características mínimas
Servidores (Web, Bases de Datos, Aplicaciones)	▪ Procesador: Intel Xeon, o AMD Opteron 2 Nucleos. ▪ Memoria Ram 8 GB. ▪ 2 Disco Duro Discos SAS 146 GB ▪ 2 Disco Duro SATA 1 TB ▪ 2 Tarjetas Ethernet de 1Gbps
Estaciones de Trabajo	▪ Procesador: Intel Core 2 Duo, o AMD. ▪ Memoria Ram 2 GB. ▪ 1 Disco Duro SATA 500 GB ▪ 1 Tarjetas Ethernet de 1Gbps
Hardware	▪ Network IDS ▪ Firewall Físico
Red	▪ Router ▪ Punto de acceso. ▪ 2 Swicth 48 puertos
Software	▪ Windows Server 2008 ▪ Versiones de Linux (Servidores

	basados en Red Hat, CentOS, Fedora ó Ubuntu) ▪ Windows 7 Professional ▪ Microsoft Office 2010
Instalación	▪ Cableado estructurado categoría 6 ▪ Conexiones eléctricas.
Servicios	▪ Conectividad a internet, Proveedor de Servicios de la región.

Fuete: El Autor

Las características descritas anteriormente son las mínimas con las que deben contar los recursos utilizados al momento de necesitar poner en operación el plan de contingencia, para información más completa y real de las características técnicas de cada uno de los componentes de la red de la Empresa, por favor remitirse al inventario de Equipos donde se relaciona detalladamente cada uno de los componentes que allí intervienen.

9.4.3 Priorización De Restauración De Servicio

Teniendo en cuenta que el Oleoducto (OAM) presta servicios de vital importancia para el país y debe estar coordinado con la red de oleoductos de Colombia, los primeros servicios a restaurar son los que tienen que ver directamente con la red de comunicaciones y Servidor Web, Servidor de Aplicaciones y Servidor de Bases de Datos, finalmente se intervendrán los dispositivos que participan en el funcionamiento interno de la Empresa.

9.4.4 Costos estimados

Tabla 9. Costos estimados

Tipo de Recurso	Descripción del recurso	Valor mensual	Valor anual
Recurso humano	Administrador IT	$ 2.000.000	$ 24.000.000
	Consultorías Especialista en seguridad informática	$ 1.000.000	$ 12.000.000
	Técnico en sistemas	$ 800.000	$ 9.600.000
Recurso tecnológico	Hardware: Servidores, computadores, impresoras, puntos de red, switches, routers, access point	$ 1.000.000	$ 12.000.000
	Software: Aplicaciones utilizadas para el manejo de información, conexiones e implementación de plataforma tecnológica	$ 500.000	$ 6.000.000
	Comunicaciones: Firewall, antivirus, tipo de conexión a internet.	$ 100.000	$ 1.200.000
			$ 64.800.000

10 CONCLUSIONES

- El Oleoducto en la actualidad no cuenta con políticas o medidas de seguridad informática o lineamientos claros para la detección, prevención y gestión de los riesgos informáticos a los que se ven expuestos dentro de la naturaleza de su actividad.

- La gestión de riesgos juega un papel importante y mediante la metodología Magerit se logra hacer una identificación clara de los activos más importantes para la organización y se realiza una valoración de riesgos.

- Se define una matriz de aplicabilidad de la política de seguridad de la información, que permitirá a todo nivel general una cultura basada en seguridad informática, con objetivos de control claros, que involucran desde la gestión de activos hasta la parte humana de la organización.

11 RECOMENDACIONES

- Se recomienda que se cree un grupo de profesionales en IT, para que implementen las salvaguardas definidas en el análisis de riesgos descritos en el capítulo anterior de este documento.

- Se recomienda que se generen revisiones periódicas de amenazas, teniendo como presente que estas, van cambiando en el tiempo y la priorización de las mismas se ve afectada por varios factores tanto internos como externos de la compañía.

- Capacitar a todo el personal, en seguridad informática e informar el papel importante, que juega cada uno de los colaboradores de la compañía.

12 BIBLIOGRAFÍA

Aguilera López, Purificación. Seguridad Informática, Citado por Galeano Villa, Jorge. Protocolo de políticas de seguridad informática para las universidades de Risaralda. [En línea]. Colombia: Universidad Católica de Pereira. 2013. Disponible en https://docplayer.es/5605322-Protocolo-de-politicas-de-seguridad-informatica-para-las-universidades-de-risaralda-jorge-luis-galeano-villa-cristian-camilo-alzate-castaneda.html

Almanza Junco, Andrés. Tendencias 2014 encuentra nacional de seguridad informática. [En línea]. Colombia: Revista Sistemas. 2014. Disponible en: http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-131/item/164-tendencias-2014-encuesta-nacional-de-seguridad-inform%C3%A1tica

Bastidas, Henry. ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN [En línea]. Colombia: Universidad Nacional Abierta y A distancia UNAD. 2014. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2668/5/763233713.pdf

Colombia. MinTics. Gobierno en linea Decreto 2693 de 2012. [En línea] 21 de Diciembre de 2012. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aafiles/eb0df10529195223c011ca6762bfe39e/decreto-2693-de-2012.pdf

Cortes, Diana. METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001 [En línea]. Colombia: Universidad EAN. junio 2012. p. 29. Disponible en https://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2&isAllowed=ydatateca.unad.edu.co/.../leccin_17_aspectos_jurdicos_de_la_norma_iso_.

El portal de ISO 27001. ISO 27000.es, [En línea]. Colombia: Portal ISO 27001. 2014. Disponible en http://www.iso27000.es/sgsi

España. Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (Octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España.

García, Alfonso, Hurtado, Cervigon, Seguridad Informática ED. 11: Informática y comunicaciones. 2011

Governance Institute. redyseguridad. [En línea] 4 de Diceimbre de 2013. Disponible en

http://redyseguridad.fip.unam.mx/proyectos/cobit/seccion_informativa/pdfscobit/resumen_ejecutivo.pdf.

http://www.seguridad.unam.mx/descarga.dsc?arch=2776.

Markus, Erb. Gestión de riesgo en la seguridad informática [En línea]. Suiza: amenazas y vulnerabilidades. 2003. Disponible en https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Reyes, Alejandro. Unam_Cert. [En línea] 30 de Agosto de 2013.] disponible en

Seguridad Inforatica. Seguridad . [En línea] 13 de Mayo de 2012. 13 de Agosto de 2013. Disponible en https://seguridadinformaticaufps.wikispaces.com/page/history/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos.

Solarte, Francisco. Datateca unda. [En línea] 20 de Frerero de 2012.Disponible en

Tamayo, Jhnny. Plan de contingencia informático [En línea]. Colombia: Universidad Nacional de Colombia Sede Manizales. 2003. Disponible en http://bdigital.unal.edu.co/57872/1/plandecontingenciasinformatico.pdf