ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"APLICACIÓN DE LA NORMA ISO 27001 EN LOS PROCESOS QUE SE REALIZAN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA EMPRESA PETROGRADOS"

EXAMEN DE GRADO (COMPLEXIVO)

Previo la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

SONIA MONSERRATE PÁRRAGA MUÑOZ

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

Agradezco primeramente a Dios nuestro ser supremo por concederme la grandeza de vivir para cumplir esta meta, a mis dos hermosos hijos Manolito y Alejandrito quienes han sido mi inspiración de fuerza y dedicación, a mi esposo Manuel Ponce por su apoyo incondicional en cada una de las etapas de mi formación profesional, a mis padres por haber hecho de mí una persona perseverante en mis decisiones y por la constante motivación.

Gracias!

DEDICATORIA

Dedico este logro a mis hijos Manolito y Alejandrito, como símbolo de superación, dedicación y muestra de que todo es posible cuando uno se lo propone. A mi esposo Manuel Ponce por su comprensión y apoyo incondicional. A mis papis Zonia y Guillermo por ser por sus consejos y apoyo incondicional.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenin Freire

DIRECTOR DEL MSIA

_____

Mgs. Laura Ureta

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

_____

Mgs. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

Un Sistema de Gestión de la Seguridad de la Información, es la representación de la importancia de la manipulación de la información en una Empresa, la Norma ISO/IEC 27001:2013, emplea controles adaptables a Instituciones sin importar la funcionalidad de las mismas.

Es así que la presente investigación se basa en la aplicabilidad de controles estipulados en la Norma ISO/IEC 27001:2013, cuyos controles han sido clasificados desde la concepción propia de la Empresa Petrogrados, generando la implementación del Sistema de Gestión de la Información en el Departamento de Tecnología.

De manera que la Empresa derive sus procesos a la excelencia, salvaguardando la seguridad de la información que fluye en cada una de las operaciones que realizan los departamentos que la conforman.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

APU: Análisis de Precios Unitario

CAD: Diseño asistido por computadora

IEC: Comisión Electrotécnica Internacional

ISO: Organización Internacional de Normalización.

PHVA: Modelo de procesos (Planificar, Hacer, Verificar, Actuar)

SGSI: Sistema de Gestión de Seguridad de Información.

.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad la seguridad de la información ha dado un crecimiento considerable, debido a fluidez de la misma en todos los ambientes ya sean físicos o lógicos. Además es notorio el crecimiento de los sistemas de información en las instituciones con la finalidad de automatizar la diversidad de procesos que generan. Sin poder limitar este crecimiento es necesario que las Empresas e Instituciones consideren lo valioso que es este activo, ya que sin una verdadera política de manipulación de la información puede deteriorarse o distorsionarse causando pérdidas y daños que en ocasiones son irremediables para una Empresa, basándose en estas problemáticas se han creado estándares para mejorar el tratamiento de la información, desde una reglamentación de accesibilidad o manipulación de un empleado, hasta la regulación del medio físico en el cual genera la información y es transformada.

Estos conceptos son estandarizados y normados, la Empresa Petrogrados, en fin de entregar un servicio de calidad, adopta la NORMA ISO/IEC 27001:2013 en el Departamento de Tecnología, tomando de referencias controles establecidos en esta norma y que engloban diversas directrices

necesarias en la seguridad de la información sin dejar a un lado la confidencialidad, la disponibilidad y la integridad de la misma.

El apoyo de la Dirección de la Empresa es primordial ante la aplicabilidad de la norma, así como también el compromiso y empoderamiento de los Directores Departamentales ante el cambio referente en los procesos convencionales y en cómo se ha manipulado la información en la Empresa, adoptando políticas de seguridades salvaguardando la seguridad de la información, logrando así ver que procedimientos no se están ejecutando de una forma correcta sin caer en un mal uso de los recursos físicos y lógicos de la Empresa.

La continuidad en la mejora, con el fin de alcanzar la calidad en los servicios brindados, es un lema que los empleados de la Empresa Petrogrados deben de plantearse en cada una de las actividades que realizan cotidianamente en la misma, tomando conciencia de la importancia de la seguridad de la información para lograr así, una verdadera aplicabilidad de la Norma para alcanzar en un futuro una certificación.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

La empresa Petrogrados, en su amplio desenvolvimiento en la elaboración y distribución de materiales pétreos y construcción, conlleva a que el flujo de la información sea circunstancial en los procesos que realizan. La seguridad de un activo, es uno de los ejes primordiales de una organización, es así que la información involucra un activo de mucha importancia por no decir el más importante de cualquier institución ya sea esta de diversa funcionalidad o naturalidad.

Es necesario para una organización, estar a la vanguardia tecnológica con el fin de innovar los procesos y brindar un mejor servicio, pero se debe de cambiar la perspectiva en relación a la protección de la información que manipulan ya que los avances tecnológicos, son una amenaza latente que tienen las organizaciones al momento de proteger la información siendo una lucha cotidiana que en ocasiones no se la realizada de forma adecuada con un Sistema de Gestión de Seguridad de la Información, la actual investigación engloba la práctica de la norma ISO 27001 para controlar y mitigar los riesgos a los que esta expuestos la seguridad de la información.

En toda organización la manipulación de la información depende de varias personas cada una de ellas con diversas responsabilidades, pero en ocasiones esto involucra no tener clara la visión de cómo debe ser tratada dicha información. Esto es un problema latente en la Empresa Petrogrados, la falta de normativas internas que regulen la seguridad de la información, explicando de manera clara lo que deben de realizar los usuarios desde la conservación de cada uno de los activos físicos y lógicos que contenga la institución.

1.2. Solución propuesta

Enmarcado en la seguridad de la información existen diversos puntos de vista, una solución factible basada en directrices reglamentadas es

la viabilidad de una normalización de los procesos, referenciados en un Sistema de Gestión de Seguridad de Información con la Norma ISO 27001, la misma que tiene inmersa controles que ayudan a direccionar de una forma equitativa los procesos de la organización para que estos puedan ser evaluados, la Empresa Petrogrados, con la aplicación de esta norma contempla una restructuración organizacional, en la cual existe mejoras en el tratamiento de la seguridad de la información.

Diseño del CICLO PDCA para la Empresa Petrogrados, en donde se establecen cada una de las fases que contemplan la Norma ISO 27001, de manera que la Empresa restructure debidamente la seguridad de la información.

La realización de un análisis de estado inicial de la Empresa Petrogrados, muestra la evidencia de como se está llevando los procesos en relación a la seguridad de la información siendo un punto de referencia para luego ir midiendo los logros y transformaciones que se realizaran a medida que se incorporen los diversos controles que contempla la norma ISO 27001.

La debida elaboración de políticas de seguridad, de manera que puedan ser evaluadas y luego distribuidas en la Empresa para que así

se pueda referir una línea u objetivo trazado para la seguridad de la información.

La implementación de esta investigación tendrá los siguientes beneficios:

- Mejoramiento de la imagen corporativa, aumentando la competitividad.
- Implementación de un Sistema de Gestión de Seguridad de la Información
- Mejorar la gestión de la seguridad de la información.
- Mejorar la participación de los empleados de la Empresa en la gestión de la seguridad de la información
- Controlar los riesgos asociados con la seguridad de la información.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Análisis de la seguridad de la información actual que emplea la empresa.

En toda empresa es esencial la fluidez de la información, aunque en ocasiones no se le dé el valor real a la misma. La información juega un rol en el crecimiento empresarial de donde se derivan los hechos desde el surgimiento hasta la sostenibilidad empresarial, es así que es necesario normalizar el comportamiento de la información desde la perspectiva de su análisis dentro de la empresa.

2.1.1. Historia Institucional

La empresa Petrogrados nació en la Ciudad de Portoviejo el treinta y uno de Enero del 2013, con un objeto social enmarcado en estudio, contratación pública y privada, y el desenvolvimiento en el ámbito de la contratación y construcción vial, fue ahí que nace la idea de crear una empresa que entregue los beneficios de todo lo relacionado a servicios de construcción y servicios pétreos en la ciudad y en el país en general, además ser una empresa capaz de brindar servicios a la comunidad en lo que respecta a mantenimiento y fiscalización en proyectos de ingeniería civil.

Al pasar del tiempo la empresa ha crecido manteniendo así en la actualidad tres áreas renombradas, en donde abarca la fabricas de asfalto, contratación de maquinarias pesadas, fabricación de adoquines, bienes raíces, contratación pública y privada. Distribuidas cada una de estas actividades desde diferentes Direcciones para que la gestión administrativa tenga una organización jerárquica funcional establecida.

2.1.2. Situación actual de la empresa.

La empresa Petrogrados desde su creación ha tenido como pilar fundamental el crecimiento institucional desde una visión

amplia, en base al desenvolvimiento propio que la identifica, logrando así transformaciones que han sido motivo del incremento de información que manipula.

Estructura Organizacional.

En la figura (Fig1), expuesta a continuación se muestra la estructura organizacional de la Empresa Petrogrados, en donde se puede visualizar de manera funcional como está representada la empresa.

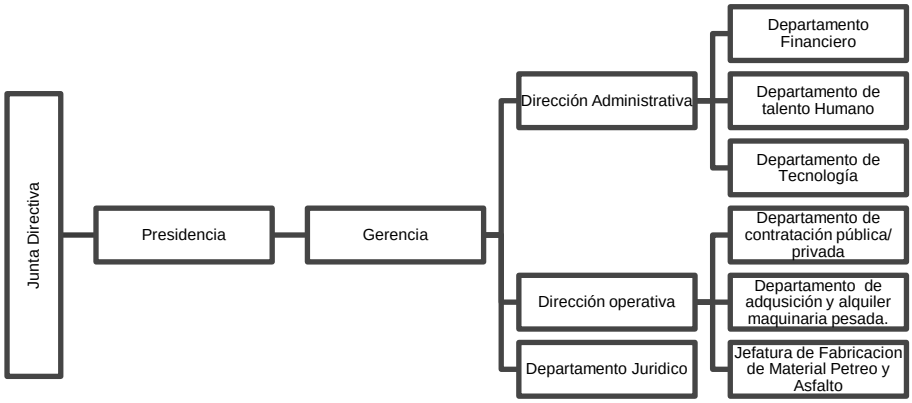

Figura 2. 1. Organigrama Funciona

La empresa actualmente desde las jefaturas departamentales, realizan diversos procesos en donde el fluido de la información es relevante a continuación se detallan cada uno de los procesos en cada una de las jefaturas.

Junta Directiva.- Es la representación de los socios, en donde se reúnen una vez por mes para discutir casos específicos, en relación a los activos físicos, términos legales y financieros de la empresa.

Gerencia.- Es la representación legal de la Empresa quien toma las decisiones de administración y gestión de los diversos procesos que ejecutan cada uno de los Departamentos, quien toma decisión en adquisición y gestión de la calidad en dichos procesos.

Dirección Administrativa.- La función de esta asignación es la de gestionar los recursos financieros, de talento humano y tecnológico representado desde las jefaturas consecutivamente, en donde cada una establece diversos procesos.

- Departamento Financiero.- La información que se manipula en este departamento se centra en los recursos financieros de la empresa.

En este departamento la información es procesada con un software contable que realiza las actividades contables de la empresa, balances, proveedores, gastos, etc.

- Departamento de Talento Humano.- La información que manipula este departamento es basada en el personal que labora en la institución.

Este departamento gestiona en un software las remuneraciones de los empleados, cuyo flujo de información es integral con el departamento financiero, para generar los respectivos roles de pagos.

- Departamento de Tecnología.- Este departamento es donde se gestiona la infraestructura de software como de hardware de la empresa.

Dirección Operativa.- La función de esta dirección es la de gestionar la funcionalidad de la empresa respecto a los servicios que brinda la misma desde las Jefaturas que representa, desde la toma de decisiones de las adquisiciones, gestión de proyectos de contratación, gestión de la fabricación de materiales pétreos y de asfalto.

- Departamento de contratación pública/ privada.- En este departamento se procesa información en base a las diversas contrataciones, es así que en este departamento tiene software gubernamental en relación a las listas y procesamientos de los cálculos de contratación, como mano de obra para realizar los

proyectos de contratación así como aplicaciones para los diseños de los mismos.

- Departamento de adquisición y alquiler de maquinaria pesada de construcción.- En este departamento se procesa información que es integrada con el departamento financiero en las cuentas de inventarios en relación a la maquinaria y utilización de las mismas.
- Departamento de Fabricación de asfalto y materiales pétreos.- En relación a la información que se procesa en este departamento consta de un registro que es derivado al departamento financiero sobre la producción que se ha generado, los gastos y lo que se ha vendido. En esta sección se lleva también inventario de los productos utilizados en la elaboración del asfalto tales como mano obra, materiales, equipos, etc.; de manera que se realice el cálculo de fabricación.

Departamento Jurídico.- En este departamento, se procesa la información legal de la empresa así como la contratación de empleados, contrataciones de obras públicas y privadas, servicios legales de la empresa. Se realizan todos los estudios de política, reglamentos o estatutos creados dentro de la empresa.

2.2. Definir el alcance del sistema de gestión de la seguridad de la información.

Al hablar del alcance del Sistema de Gestión de la Seguridad de la Información según la norma ISO/IEC 27001:2013(E):

“La organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, documentado en el contexto de las actividades globales el negocio de la organización y de los riesgos que enfrenta”. [1].

La empresa Petrogrados, dentro de su estructura organizacional contiene un Departamento Tecnológico, donde se establece la manipulación lógica de la información, el alcance del SGSI de la empresa se concentra en la seguridad de la información en base a los procesos que se manipulan a través de este departamento, en relación a los controles en de acceso físico y lógico de la información adoptando el modelo de procesos de la norma ISO/ IEC 27001:2013; que indica: Planificar, Hacer, Verificar y Actuar (PHVA); para estructurar así todos los procesos del SGSI y emprender a una mejora en la calidad en relación a la seguridad de la información manipulada.

El alcance del SGSI es basado en los objetivos de control y controles de la Norma ISO/IEC 27001:2013; A.5. Política de Seguridad, A.6.

Organización de seguridad de la información, A.7. Gestión de Activos, A.9. Seguridad Física y del entorno, A.10. Control de Acceso.

2.2.1. Seguridad de la información.

Como se cita a continuación:

“La Seguridad de la Información se define como la implementación de medidas técnicas, debidamente planificadas y organizadas con el fin de asegurar la confidencialidad, integridad y disponibilidad de su sistema de información”. [2].

“Consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; de manera que la información cumpla con las características de autenticidad, no repudio y la confiabilidad”. [1]

Confidencialidad: “Esta características es cuando la información no es disponible, comunicable y divulgable entre individuos o entidades”. [3]

Integridad: “Se caracteriza por el aseguramiento de la información durante el procesamiento, transportación u almacenamiento de la misma, de manera que se detecte si se realizaron modificaciones no autorizadas”. [3]

Disponibilidad: “Se caracteriza por el acceso de la información, ante una denegación de uso no autorizado de la misma, asegurando así la accesibilidad de la información cuando se requiera”. [3]

2.2.2. Importancia de la información.

La importancia de la información como uno de los activos con mayor ponderación en la funcionalidad de una Institución, es así que la necesidad de proteger este activo es muy importante. Actualmente el incremento de la manipulación de los Sistemas de Información para agilitar los procesos de las Empresas hacen que la información este expuesta y vulnerable; la falta de conocimiento para mitigar riesgos de ataques genera un impacto negativo en el cual una Institución puede tener pérdidas innumerables, si la información es alterada, ocasionando que la información no se pueda preservar de una forma idónea. [4].

Es necesario que las Empresas vean a este activo como un medio circunstancialmente importante para la funcionalidad y evolución de la misma.

2.3. Implementar el sistema de gestión de la seguridad de la información.

2.3.1. Política de seguridad

"La Política de Seguridad se define como la Normativa interna en donde se estipulan diversos criterios organizadamente establecidos en relación a la seguridad de la información". [5]

La Empresa Petrogrados desde la Junta Directiva estableció la Política de seguridad, la misma que está basada en el control A.5. De la Política de Seguridad de la Norma ISO 27001, cumpliendo así con los objetivos propuesto en la norma como se detalla a continuación:

En relación a este punto se establecieron los parámetros en base a la seguridad de la información desde la Implementación del SGSI en el Departamento de Tecnología de la Empresa.

Las políticas se enfocan a los controles con los cuales se va a operar en la Empresa empleando así la Seguridad Física y del Entorno, el Control de Seguridad Física y del Entorno, Control de Acceso.

En la política se refleja el compromiso de los Directivos de la Empresa en la gestión, debido a que es de mucha importancia

que estén inmersos en la toma decisiones y en cada etapa de la gestión, evaluación y mejoramiento de la calidad de la Empresa.

Es importante aclarar que la Gerencia de la Empresa está al tanto de la importancia de la continuidad en base al mejoramiento y porque no decir la implementación de más controles de la Norma 27001, y lograr el nivel de Calidad necesario para certificar.

En el proceso de diversas revisiones legales es necesario que sea aprobada la política y así también sea socializada debidamente con cada uno de los empleados de la Empresa para que concienticen varios puntos que se contemplan en la misma.

2.3.2. Control de Acceso

La accesibilidad física y lógica de los bienes de una empresa actualmente son mucha importancia para cualquier institución, sea cual sea su desenvolvimiento, debido a que la información de la Empresa no puede ser manipulada sin autorización y dependiendo el nivel o la asignación que tiene el usuario o empleado, está comprobado por estudios a nivel mundial que la manipulación no adecuada por parte de los empleados de una empresa han comprometido el funcionamiento de la misma.

Es así que la política establecida toma en cuenta generalidades que deben de acatar la Empresas en relación al acceso, privilegios y restricciones que deben operar en una Institución.

A continuación se muestran los criterios establecidos en la Norma ISO/IEC 27001:2013, en donde se exponen los diversos parámetros que han sido tomados en cuenta para establecer las políticas de seguridad y los sub – criterios para la vigencia y el cumplimiento de las mismas, de manera que puedan ser evaluados desde cada una de las responsabilidades.

A.9.2 Gestión de acceso al usuario

Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios.

A.9.2.1. Registros y des-registros del usuario

Control: La implementación de una proceso estructurado de registro y des-registro del usuario para habilitar los derechos de acceso.

Política de Seguridad: En la política seguridad se define que el Jefe de Departamento de Tecnología, es quien contenga los registros de usuarios y contraseñas que han sido asignados a las demás Direcciones.

Sub - criterio:

- Establecer la identificación de usuarios únicos, de manera que cada empleado pueda trabajar en el perfil de usuario correspondiente.

- Para acceder a la información de la base de datos se verifica que el usuario que accederá tiene autorización de la Dirección del Departamento.

- Reglamentar por escrito la entrega del usuario bajo responsabilidad del empleado.

- Mantener el registro formal de todas las autorizaciones realizadas.

- Efectuar revisiones periódicas a los pc's de la empresa con el fin de verificar alguna anomalía en relación a los usuarios.

Responsable: Dirección del Departamento de Tecnología

A.9.2.2 Provisión de Acceso al usuario

Control: La implementación de un procedimiento formal y estructurado de la provisión de acceso al usuario, para asignar o revocar los derechos de acceso de todos los tipos de usuarios a todos los sistemas y servicios.

Política de Seguridad: En la política de seguridad se establece que el Jefe del Departamento de Tecnología es quien edita, elimina, y actualiza los registros de usuarios y cuentas en sí.

Además se establece el procedimiento de para la cancelación de algún usuario e intrusión no autorizada a los mismos.

Sub – Criterio:

- Elaborar informe de cuentas que contemplan provisión de acceso.

- Eliminar cuentas de usuarios inactivas.

- El Director del Departamento de Tecnología deberá elaborar el procedimiento para la cancelación de cuentas de usuarios e intrusión no autorizada.

Responsable: Dirección del Departamento de Tecnología

A.9.2.3. Gestión de los Derechos de Acceso

Control Privilegiado: Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.

Política de Seguridad: En la política de seguridad se establece la responsabilidad de los Derechos de Accesos Privilegiados al Director de Departamento de Tecnología.

Sub – criterio:

- Establecer la identificación de los accesos privilegiados en las diversas aplicaciones así como en las bases de datos de la Empresa.

- Clasificar los tipos de privilegios de acceso que se identificaran en la seguridad de la información de la empresa.

- El Director del Departamento de Tecnología entregará los privilegios a los usuarios con cartas de responsabilidades de los mismos.

Responsable: Dirección del Departamento de Tecnología.

A.9.2.4 Gestión de Información de Autenticación secreta de Usuarios

Control: Se debe controlar la asignación de la información de autenticación secreta de los usuarios mediante un proceso de gestión formal.

Política de Seguridad: En la política de seguridad se establece que es responsabilidad del Director del Departamento de Tecnología el registro y asignaciones de autenticaciones secretas de los usuarios.

En la política se establecen las responsabilidades del usuario en relación a la autenticación entregada por el Departamento de Tecnología

Sub – Criterio:

- Establecer un registro detallado y con firma de responsabilidad del tipo de autenticación por parte del usuario.

- Carta de responsabilidad, en relación a la asignación entregada.

Responsable: Dirección del Departamento de Tecnología, Usuarios.

A.9.2.5. Verificación de los Derechos de acceso de los usuarios

Control: Los propietarios de los activos deben de verificar los derechos de acceso de los usuarios a intervalos regulares.

Política de Seguridad: En la política se establece las responsabilidad que debe de tener el usuario en relación a sus accesos.

El jefe de Departamento de Tecnología debe de monitorear los accesos de los usuarios

Sub – Criterio:

- El Director del Departamento de Tecnología debe de tener un reporte de monitorio de los derechos de accesos de los usuarios.

- Debe de informar a la Gerencia cualquier anomalía en relación a la violación de algún derecho de acceso.

Responsable: Dirección del Departamento de Tecnología, Usuarios.

A.9.2.6 Retiro o ajustes de los Derechos de Acceso.

Control: Los derechos de acceso a todos los trabajadores y terceros a la información a las instalaciones de procesamiento de la información deber ser retirados al termino de empleo, contrato o acuerdo, o ajustado luego de un cambio

Política de Seguridad: La política especifica que si un empleado es retirado de la empresa o cambiado a otro departamento debe de indicarse al Departamento de Tecnología dicho cambio, para ejecutar los debidos procesos de reubicación o ajustes a los derechos de acceso.

Sub – Criterio:

- Documentación de comunicación del cambio de usuarios emitida por Gerencia.

- Documentación del proceso de cambio retiro o ajustes de los Derechos de Accesos, legalmente registrada por el empleado y el Director de Tecnología.

- Documentación de reasignación del rol de usuario a la persona indicada por la Gerencia.

Responsable: Departamento de Tecnología, Gerencia

A.9.3 Responsabilidad del usuario

Concientizar en los usuarios las responsabilidades de salvaguardar la autenticación de la información

A.9.3.1 Uso de información secreta de autenticación

Control: Aplicación de las buenas prácticas de la organización sobre el uso de la información secreta de autenticación

Política de Seguridad: La política de seguridad establece que los usuarios que tienen autenticación de claves secretas será bajo responsabilidad juramentada de manera que se personifique la manipulación de la misma.

Sub – Criterio:

- Documentación que respalde la designación de autenticación por parte del Departamento de Tecnología.

Responsable: Director del Departamento de Tecnología, Usuario.

A.9.4 Control de acceso a sistemas y aplicaciones

Es necesario que se evite el control de acceso no autorizado a los sistemas y las aplicaciones de la Empresa

A.9.4.1 Restricciones de acceso

Control: Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso

Política de Seguridad: La Dirección deberá emitir un informe de los accesos no autorizados en las restricciones, mediante el continuo monitoreo de los accesos realizados por los usuarios.

Se tomaran medidas correctivas ante cualquier anomalía en los accesos no autorizados.

Sub – Criterio:

- Informes por parte de la Dirección del Departamento de Tecnología.

- Accesos no Autorizados medidas correctivas.

Responsables: Director del Departamento de Tecnología, Usuarios.

2.3.3. Gestión de los activos

Activo: Cualquier cosa que tenga valor para la Organización [1]

Dentro de la empresa es necesario especificar la importancia de las responsabilidades en de los usuarios en relación a los activos, estos deben de estar bien definidos desde su usabilidad hasta las características que los representan a cada uno, haciendo la manipulación más oportuna y responsable.

Para la realización de la conformidad de una empresa se encuentran identificados la distribución de activos, desde la concepción antes expuesta los activos reflejan propiedades de una empresa, ya sean estas físicas o lógicas.

Para un mejor análisis se van a dividir los activos físicos (hardware) y activos lógicos (software), de la Empresa de manera que se pueda diferenciar los respectivos criterios que estarán inmersos en el control de los activos.

En las tablas a continuación se expone el inventario la estructura de los activos físicos y lógicos que posee la Empresa.

Inventario de activos físicos (hardware).

1. **Descripción del hardware:** 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Recepción de la Empresa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Recepcionista de la empresa

2. **Descripción del hardware:** 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Dirección Operativa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Director Operativo

3. **Descripción del hardware:** 1 PC de escritorio

Marca: Inspiron

Modelo: 36470

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Departamento Jurídico.

Fecha de adquisición: 10 de Septiembre del 2015

Responsable: Jefe Departamental

4. **Descripción del hardware:** 3 PC de escritorio

Marca: Inspiron

Modelo: 3600

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Departamento Financiero

Fecha de adquisición: 10 de Septiembre del 2013

Responsable: Departamento Financiero: Jefe Departamental, Contadora, Proveeduría.

5. **Descripción del hardware:** 2 PC de escritorio

Marca: Inspiron

Modelo: 3600

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Departamento de Talento Humano.

Fecha de adquisición: 10 de Septiembre del 2013

Responsable: Jefe Departamental, Secretaria.

6. **Descripción del hardware:** 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Recepción de la Empresa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Gerencia; Secretaria de Gerencia.

7. Descripción del hardware: 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Recepción de la Empresa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Presidencia

8. Descripción del hardware: 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Recepción de la Empresa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Director Administrativo

9. Descripción del hardware: 2 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Recepción de la Empresa

Fecha de adquisición: 15/mayo/ 2014

Responsable: Departamento de adquisición de maquinaria; Jefe departamental, asistentes de inventarios

10. Descripción del hardware: 3 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Departamento de Contratación Pública.

Fecha de adquisición: 15/mayo/ 2014

Responsable: Jefe Departamental, Ingeniero 1, Ingeniero 2.

11. **Descripción del hardware:** 1 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Jefatura de Fabricación de Asfalto

Fecha de adquisición: 15/mayo/ 2014

Responsable: Jefe Departamental

12. **Descripción del hardware:** 3 PC de escritorio

Marca: Inspiron

Modelo: 3647

Procesador: CORE I3 4160 3.40GHZ DE 2DA GENERACION

Memoria: 4GB de Memoria un solo Canal DDR3 a 1600MHz

Disco Duro: SATA de 1TB 7200 RPM (6.0 Gb/s)

Sistema Operativo: Windows 7 (no licenciado)

Ubicación: Departamento de Tecnología

Fecha de adquisición: 15/mayo/ 2014

Responsable: Director de Departamento de Tecnología, asistente técnico, administración de redes.

13. Descripción del hardware: 1 Servidor

Marca: IBM

Modelo: System X3200M2.

Procesador: Intel Xeon E3110 / 3 Ghz.

Memoria: 1 GB/8 GB (max.)

Disco Duro: 1x Serial ATA – Integrado Serial ATA - 300

Sistema Operativo: IBM ServerGuide, IBM Director

Ubicación: Departamento de Tecnología

Fecha de adquisición: 23/mayo/ 2013

Responsable: Director del Departamento de Tecnología

Inventario de Activos lógicos de la Empresa (Software)

1. **Nombre de la Herramienta:** Windows 7

Descripción de la Herramienta: Sistema operativo para el funcionamiento del equipo.

Aporte del Trabajo: Es el Sistemas operativo con él se manejan los computadores de escritorio de la empresa.

Equipo: En totalidad 17 computadores contienen esta herramienta. Esta herramienta no es licenciada en la Empresa

Ubicación: En cada computador de escritorio que tienen los diferentes departamentos de la empresa.

Responsable: Los empleados de la empresa que manejan los diferentes computadores de escritorio.

2. **Nombre de la Herramienta:** Microsoft Office 2010

Descripción de la Herramienta: Contiene utilería de ofimática en la cuales se desarrollan diversas actividades como redacciones, creación de hojas de cálculo, presentaciones, etc

Aporte del Trabajo: Es de gran aporte puesto que en relación a la ofimática necesaria para la gestión administrativa de cada uno de los departamentos se necesita documentar actividades.

Equipo: En totalidad 17 computadores contienen esta herramienta. Esta herramienta no es licenciada en la Empresa

Ubicación: En cada computador de escritorio que tienen los diferentes departamentos de la empresa.

3. **Nombre de la Herramienta:** Génesis Contable

Descripción de la Herramienta: En esta herramienta se realizan los procesos contables de la empresa, balances, roles de pago, cuentas, gastos proveedores, etc.

Aporte del Trabajo: Esta herramienta es muy importante para la Empresa ya que ayuda a determinar el balance financiero de la misma.

Equipo: El Génesis Contable lo portan los tres computadores de escritorio del Departamento Financiero, Jefatura de Fabricación de asfalto, Departamento de Adquisición y maquinaria.

Ubicación: Departamento Financiero, Jefatura de Fabricación de asfalto, Departamento de Adquisición y maquinaria.

Responsable: Los responsables de cada uno de estos Departamentos el personal que labora en los mismos.

4. **Nombre de la Herramienta:** Auto CAD

Descripción de la Herramienta: Esta herramienta es de diseño de ingeniería, plano, dimensiones, etc., de utiliza ayuda al momento de proyectar una obra para contratación.

Aporte del Trabajo: La utilización de esta herramienta se basa en la elaboración de los diferentes diseños arquitectónicos y de infraestructura para construcción.

Equipo: Esta herramienta la utilizan los equipos del Departamento/Privada.

Ubicación: Departamento de Contratación pública / privada

Responsable: Los empleados que laboran en el Departamento de Contratación Pública/ Privada.

5. **Nombre de la Herramienta:** APU

Descripción de la Herramienta: Esta herramienta es de análisis de precio unitario, en donde realizan los costos de una construcción.

Aporte del Trabajo: Esta herramienta es de gran ayuda para la elaboración de los presupuestos ante una contratación sea esta pública o privada

Equipo: Esta herramienta la utilizan los equipos del Departamento/Privada

Ubicación: Departamento de Contratación pública / privada

Responsable: Los empleados que laboran en el Departamento de Contratación Pública/ Privada.

6. **Nombre de la Herramienta:** Centos 5.0.

Descripción de la Herramienta: Sistema operativo del Servidor.

Aporte del Trabajo: Esta herramienta es de mucha importancia pues gracias a ella se realiza la administración del servidor de Base de Datos

Equipo: La utiliza el servidor que se encuentra en el Departamento de Tecnología

Ubicación: Departamento de Tecnología

Responsable: Analista de tecnología – Administrador del Servidor.

7. **Nombre de la Herramienta:** Mysql.

Descripción de la Herramienta: EL mysql Worbrench es un herramienta que ayuda a modelar una base de datos

Aporte del Trabajo: Es de mucha importancia de la empresa debido a que la Base de Datos contiene el almacenamiento de los datos

Equipo: La utiliza el servidor que se encuentra en el Departamento de Tecnología

Ubicación: Departamento de Tecnología

Responsable: Analista de tecnología – Administrador del Servidor.

CAPÍTULO 3

ANALISIS DE RESULTADOS

3.1. Auditorías Internas

Las auditorias son un mecanismo para evaluar la situación actual en base a la funcionalidad de los procesos que ejerce una organización o Institución.

La auditoría aplicada en el Departamento de Tecnología de la Empresa Petrogrados, mostró una visión global de la funcionalidad del Sistema de Gestión de la Seguridad de la Información, tomando en cuenta que estos parámetros evaluados, ayudan a determinar

diversos factores en los que no se está procesando debidamente la información.

3.1.1. Metodología de la valoración de riesgos.

Desde el análisis de la información manipulada por la Empresa, se realizó la clasificación de la información en base a la confidencialidad, Integridad y Disponibilidad.

Desde la Norma ISO/IEC 27001: 2013, se definen los controles de la Organización de Seguridad de la información los mismos que serán tomados en cuenta para la auditoria interna creando así una valoración es las funcionalidades y el mecanismo de uso que se está realizando.

Confidencialidad: "Característica para determinar el estado de la información, si está disponible o no, si no ha sido revelada a individuos". [1]

Tabla 1: Criterios de Clasificación de la Disponibilidad de la Información

Criterio	Descripción
0	La información que puede ser manipulada sin ninguna restricción por cualquier usuario, sea empleado de la Empresa o no, pero que esté debidamente registrado.

1	Información que puede ser manipulada por todos los empleados de la Empresa, para su conocimiento y utilización, si en caso que sea divulgada dicha información no ocasione riesgos a la Empresa.
2	Información que solo puede ser manipulada por un grupo de empleados de la Empresa, de forma que sus uso sea necesario para realizar su trabajo, cuya divulgación o uso no autorizados podría ocasionar pérdidas o riesgos en la Empresa.
3	Información que solo puedes ser manipulada y conocida por un grupo seleccionado de empleados de la Empresa, como Gerencia, Presidencia, Direcciones y Jefaturas Departamentales.

Integridad: "Característica propia para la protección del estado de la información"**.** [1]

Tabla 2. Criterios de Clasificación de la Integridad de la Información

Criterio	**Descripción**
0	Manipulación y modificación sin autorización con fácil reparación, o no influye la gestión operativa de la Empresa.
1	Manipulación y modificación sin autorización que pueda repararse pero ocasionaría riesgos en la gestión operativa de la Empresa.
2	Manipulación y modificación sin autorización que sea difícil de repararse, pero podría ocasionar perdidas en la gestión operativa de la Empresa

3	Manipulación y modificación sin autorización que sea difícil de no se pueda reparar, pero ocasionaría perdidas en la gestión operativa de la Empresa

Disponibilidad: "Característica en donde la información es accesible y utilizable por solicitud de una entidad autorizada".[1].

Tabla 3. Criterios de Clasificación de la Disponibilidad de la Información

Criterio	**Descripción**
0	La inaccesibilidad no afecta la gestión operativa de la Empresa.
1	La inaccesibilidad permanente durante dos días, podría ocasionar pérdidas significativas para la Empresa
2	La inaccesibilidad permanente por más de diez horas, podría ocasionar pérdidas significativas a la Empresa.
3	La inaccesibilidad permanente por más de media hora, podría ocasionar pérdidas significativas a la Empresa.

Para realizar la auditoria se tomaron criterios de valoración alto, medio, bajo en relación con la Confidencialidad, Integridad y Disponibilidad, con el fin de poder clasificar las amenazas y las

vulnerabilidades que se presentan. Basándose en los criterios antes mencionados se derivan las siguientes concepciones:

Tasación: Consiste en una evaluación basada en la valoración de una estimación. [6]

Análisis de riesgo: La utilización sistemática de la información con la finalidad de identificar fuentes y realizar la estimación de riesgos. [1]

Valoración del riesgo: El procesamiento de la información desde un análisis global y evaluación de riesgos. [1]

Tabla 4 Tabla de tasación

Activos	**Tasación**			
	C	**I**	**D**	**Tota**
Servidor de base de datos	A	A	A	A
Equipo de escritorio	A	A	A	A
Sistemas operativos	A	A	A	A
Software	A	A	A	A

Tabla 5. Tabla de Valoración de los Riesgos

Amenazas	Probabilidad Ocurrencia	Vulnerabilidad	Posible Explotación de Vulnerabilidad
- Hackers	B	Software Desactualizado	B
- Virus	M	Falta de actualización y licencias de antivirus	M
- Seguridad física	A	El acceso a donde está el servidor, no es por registro de autenticación biométrica o tarjeta.	A
- Virus	A	Software no licenciado ni antivirus licenciado. Falta de antivirus licenciado.	M
- Marlware	A	Falta de Capacitación al usuario.	M
- Seguridad de acceso	B	Falta de Capacitación al personal a la asignación de claves y de inicio de sesión.	B
- Seguridad Física	M	Falta de Capacitación al personal en relación a la gestión del área física en el sé que desenvuelve.	B
- Seguridad lógica	A	Sistemas operativos no licenciados	A

- Seguridad lógica	A	Sistemas operativos no licenciados	A

C: Confidencialidad
I: Integridad
D: Disponibilidad

A: Alta
M: Media
B: Baja

3.2. Acciones Correctivas.

Al indicar las acciones correctivas necesarias que debe de optar la empresa se reflejan en los criterios expuestos a continuación:

- Se debe de tener en cuenta la responsabilidad de la Dirección del Departamento de Tecnología debido a que la mayoría de las vulnerabilidades fueron más hacia los activos de software en relación a los sistemas operativos que manejan en los computadores de escritorio en la institución no están debidamente registradas las licencias, por lo que genera un riesgo a la información ya que esta tiende a estar vulnerable ante diversos ataque y robos de la información, es necesario que se informe desde el alcance de amenazas a la Gerencia para que se tome medidas al respecto y se reorganice una estructura de software que garantice la confidencialidad, integridad y disponibilidad de la información.

- Es necesario que continuamente la gerencia monitorice los reportes emitidos por la Dirección del Departamento de Tecnología de manera que pueda ver si se están cumpliendo debidamente con los procesos y procedimientos reglamentados en las políticas de seguridad asegurando el Sistema de Gestión de la Seguridad de la información

CONCLUSIONES Y RECOMENDACIONES

CONCUSIONES

1. La información es prevista como un activo valioso para toda Empresa, desde mi concepción, toda organización debe proteger este activo para así asegurar la gestión, que caracteriza la debida funcionalidad de la misma, desde esta premisa puedo indicar que esta la Norma ISO/IEC 27001:2013, es un estándar que se basa en la seguridad de la información, y es relevante indicar que ahora las empresas cuentan con esta norma para mejorar la gestión de la información.

2. La adaptación de la Norma ISO/IEC 27001:2013 en el Departamento de Tecnología, ayudo a verificar ciertos procesos que no se estaban ejecutando debidamente, logrando así mejorar la funcionalidad de la Empresa.

3. La Empresa Petrograds, a pesar de ser joven institucionalmente, realiza varios procesos en que es de mucha importancia, la disponibilidad de la información es así al realizar la auditoria interna se pudo constatar que en ocasiones por tener esta disponibilidad no se realiza el debido tratamiento de la información dejando a un la lado la integridad de la misma.

RECOMENDACIONES

1. En todo proceso de cambio es necesario el respaldo de las máximas autoridades de una Organización, para que pueda ejecutarse cada una de las fases de este cambio.

2. El acompañamiento de la Gerencia es necesaria, puesto que es el responsable directo ante cualquier toma de decisiones, siendo necesario ante la implementación de una norma explicar de forma clara el alcance de la misma y la necesidad de este acompañamiento.

3. Es recomendable que se mantenga informado continuamente a la Dirección o Gerencia de cada uno de los acontecimientos o controles que se estiman a implementar en el Sistema de Gestión de la Seguridad de la información, de manera que la Gerencia tenga conocimiento siempre de las acciones tomadas.

4. El Departamento de Tecnología de la Empresa Petrogrados, asumió junto con la Presidencia y la Gerencia entrar en proceso de mejora continua, con el fin de acreditar en cada uno de los controles que contempla la NORMA ISO/IEC 27001:2013, mi recomendación es no desmayar ante esta posibilidad debido a que los cambios han sido notorios desde cómo se empleaba la seguridad de la información antes en relación a como se lo realiza ahora.

BIBLIOGRAFÍA

[1] I. S. Organization, Information tecnology - Security techniques - Information security management systems - Requerimients, Segunda ed., ISO/IEC 27001:2013, 2013.

[2] E. Mifsud, «Observatorio Tecnologico,» 26 mayo 2012. [En línea]. Available: http://recursostic.educacion.es/observatorio.

[3] D. d. J. y. A. Publica, «Soluciones de Seguridad Global,» 21 Abril 2010. [En línea]. Available: www.belt.es.

[4] M. I. LADINO, P. A. VILLAS y A. M. LÓPEZ, «Fundamentos de iso 27001 y su aplicación en las empresas,» *Scientia et Technica,* vol. 1, nº 47, pp. 334-339, Abril 2011.

[5] isotools, «Isotools,» 2014. [En línea]. Available: www.isotools.org.

[6] C. Alberts y A. Dorofee, Managing information security, Longman: Addison-Wesley, 2002.