ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"EMPLEO DE LA NORMA ISO 27001 PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA EMPRESA ROCASOLIDA CONSTRUCCIONES S.A."

EXAMEN DE GRADO (COMPLEXIVO)

Previo la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MANUEL ALEXANDER PONCE TUBAY

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

Al ser supremo nuestro Dios, por haberme dado la fuerza y voluntad necesaria para culminar una etapa más en mi vida, a mis adorables hijos Manuel Alexander y Manuel Alejandro quienes son mi fortaleza y dedicación cada día de mi vida, a mi esposa Sonia Parraga por el apoyo que me brinda incondicionalmente cada día en la diferentes etapas de vida profesional, a mi padre Manuel Vicente y Madre Vilma por su motivación y haberme guiado siempre por el buen camino ya sea en el ámbito personal y profesional.

Gracias!

DEDICATORIA

Este triunfo se le dedico a mis hijos Manuel Alexander y Manuel Alejandro quienes son mi fortaleza y dedicación cada día de mi vida, a mi esposa Sonia Parraga por el apoyo incondicional que siempre me brinda todos los días, a mis padres Manuel y Vilma por el soporte que me han brindado en cada una de las etapas de mi vida.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR DEL MSIA

Mgs. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

Las técnicas de seguridad de la información en una empresa, establece el manejo de los diferentes procesos que la conforman, la Norma ISO/IEC 27001:2013, maneja los diferentes controles que son adaptables a cualquier organización e institución sin importar los servicios que brindan.

Esta investigación se basa en el establecimiento de los diferentes controles que se encuentran determinados en la Norma ISO/IEC 27001:2013, los cuales se clasificaron en base a las diferentes concepciones de la empresa Rocasolida Construcciones S.A., para de esta forma lograr la implantación de Técnicas para el aseguramiento de la Información adecuadas para el Departamento de Tecnología.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CAD: Diseño asistido por computadora

IEC: Comisión Electrotécnica Internacional

ISO: Organización Internacional de Normalización.

PC: Computador de Escritorio

S.O: Sistema Operativo

.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el mundo actual en el que vivimos la información es el activo más importante en una empresa, cada día se encuentra más vulnerable a ataques no tan solo desde el exterior sino que también internamente, debido a los avances tecnológicos hace que explotar un vulnerabilidad en estos días se pueda realizar tan fácilmente, lo que conlleva a que cualquier persona con pocos conocimientos informáticos puede sacarle provecho a las vulnerabilidades que muchas organización la tienen y que muchas veces las auditorias que se realizan en las mismas no las detectan, estas debilidades en la empresa ocasiona la perdida de información la cual en la mayoría de casos es primordial para desarrollo y progreso en toda institución la cual debe estar siempre disponible, confiable y no debe ser alterada a, por consiguiente la alteración o modificación de la ella puede causar daños irremediables a la entidad, mermando así la fluidez económica de la empresa. Estas concepciones son normalizadas y estandarizadas, Rocasolida Construcciones, con el fin de mejorar la calidad en los servicios que brinda, se acoge la NORMA ISO/IEC 27001:2013 en el Departamento de Tecnología, optando como referencia los controles establecidos en la norma los mismos que comprenden las diferentes preceptos necesarios en la

seguridad de la información para que misma sea confiable, disponible e integra en la organización.

Es fundamental la ayuda de la dirección de la empresa, de los directores de departamentales y de los empleados para el mejoramiento de los diferentes procesos y como se ha llevado el manejo de la información en la organización, estableciendo funciones y responsabilidades a la seguridad de la información, políticas de seguridad al acceso de la información y mejorando los términos condiciones y procesos al momento de la contratación de los empleados.

La mejora en cada uno de los servicios que brinda la empresa Rocasolida Construcciones, es la meta que tienen cada día todos los empleados de la organización, tomando en consideración en activo más importante que tiene la empresa que es la información salvaguardarla y protegerla logrando así, el emplear la norma para de esta forma logar en lo posterior una certificación de la empresa.

CAPÍTULO 1

GENERALIDADES

1.1. Problematización

Rocasolida Construcciones S.A una empresa dedica a obras de ingeniería civil y fabricación de asfalto, en la actualidad toda organización de maneja su información de forma digital y Rocasolida no es la excepción, por ello es de suma importancia asegurar este activo que es uno de los más importantes de una empresa.

La información en la empresa se encuentra muy vulnerable debido a que la misma no cuenta con el establecimiento de políticas de seguridad de la información, por lo cual es susceptible al robo de la

información, lo cual podría representar pérdidas económicas en la misma.

La organización de la seguridad de la información en la empresa no se encuentra debidamente establecida en relación a las responsabilidad y funciones que ejercen los empleados, es necesario establecer todas las tareas que se realizan en la institución, lo que conlleva a que no se mantenga el respectivo contacto de los superiores con sus subordinados lo cual implica una descoordinación total de toda la información que se maneja en la empresa.

El recurso humano con que cuenta la empresa no presenta un proceso de contratación adecuado, debido a que no se realiza la verificación de los antecedentes de los candidatos a los puestos de trabajo, también se pudo constatar que en la elaboración de sus contratos no existen clausulas sobre el manejo, seguridad y confidencialidad de la información que se maneja la empresa.

En la organización no se cuenta con inventario de activos de los equipos y maquinarias que posee, lo que ocasiona que no exista un control de quien o cuales operan los diferentes activos de la empresa.

El acceso a los recursos de la red no se encuentran debidamente establecidos debido a que no existen políticas para el control de acceso a estos, lo cual en ocasiones conlleva que se los diferentes

equipos que se encuentran compartidos en la red no tengan el uso adecuado.

Los accesos a las instalaciones de la organización no cuentan con la respectiva seguridad y más aún el acceso al departamento tecnológico, la entrada al mismo no cuenta con las garantías mínimas como lo establecen los estándares.

1.2. Solución propuesta

Para que la empresas cuente con la debida seguridad de la información, como una solución factible se establecerán políticas de seguridad para en manejo de la información que posee la empresa las que deberán ser definidas, aprobadas, publicadas y comunicadas por la gerencia y quedar establecidas para el respectivo manejo de la información en la organización.

Se deben establecer las funciones y responsabilidades de la seguridad de la información de la empresa, la segregación de tareas para que no exista la oportunidad de que la información sea alterada o modificada por personal no autorizado o el mal uso de la misma, establecer una debida comunicación entre los superiores y sus subordinados los mismos que deben tener claro a quienes tendrá que

rendirles informes sobre la información que cada uno de ellos tienen a cargo.

La forma de contratación del personal que labora en empresa se debe regir a lo establecido en las leyes y regulaciones, a la ética y las políticas establecidas en la organización para el manejo y seguridad de la información.

Realizar un inventario de activos el mismo que le permitirá establecer a la empresa todo el equipamiento y maquinaria con que cuenta y establecer quien o quienes son los responsables del uso y manejo de los mismos, logrando un mejor control de ellos.

Se debe considerar establecer políticas de acceso a las instalaciones de la empresa y especial al departamento de tecnológico, en el cual se deben mejor el acceso implementándole mejoras a la seguridad de acceso.

Establecer las respectivas políticas de acceso a los usuarios, para darle el debido uso a los diferentes servicios con lo que cuenta la red de la empresa, y de esta forma brindarle un mejor aseguramiento de la información.

Los beneficiarios que estarán involucrados en esta investigación se enlistan a continuación:

- Con un esquema de seguridad de la información la empresa mejora su imagen, lo cual le permitirá tener una mayor competencia con empresas a nivel local y nacional, aumentando su competitividad en el mercado.
- Con la implementación de políticas de seguridad se tendrá un mejor manejo de la información de la empresa
- Mejoras en el proceso de contratación del recurso humano de la empresa
- Se tendrá un mejor control y operación de los activos que posee la empresa
- Se establecerán políticas para control y acceso a las instalaciones y a los diferentes departamentos al personal no autorizado.
- La empresa tendrá un manejo adecuado de los servicios de red con los que cuenta, estableciendo políticas de acceso y seguridad a los usuarios

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Estudio del estado actual de la seguridad de la información de la empresa.

En la actualidad la mayoría de las empresas en nuestro medio le dan poca importancia al manejo y seguridad de la información, la cual es uno de los pilares fundamentales para mejoramiento y desarrollo de una organización, la cual mediante un estudio interno de la institución se normalizara el manejo y seguridad de la información, la cual es uno de los activos que más se debe de proteger para el progreso y mejora de los diferentes servicios que brinda la institución.

2.1.1. Antecedentes Históricos de la Empresa

Rocasolida Construcciones S.A. fue constituida el 22 de Diciembre del 2009 en la ciudad de Portoviejo, la cual inicio con el objetivo de social de la construcción, mantenimiento, estudio y fiscalización de redes eléctricas, proyectos eléctricos e hidroeléctricos y obras de ingeniería civil, la empresa a desarrollo diferentes tipos proyecto referentes con los diversos servicios que brinda tanto en el sector público como en el privado.

En la actualidad Rocasolida Construcciones S.A. se ha constituido en una de las más reconocida a nivel la provincia de Manabí, por los diferentes servicios que presta, como la construcción de carreteras, alquiler de maquinarias, la elaboración y ejecución de proyecto eléctricos e hidroeléctricos y la producción de asfalto de primera calidad para calles y vías de la provincia, logrando la adquisición de contratos con entidades públicas y privadas. Cada una de estas actividades se encuentra representada por un jefe departamental para la administración de las jerarquías funcionales establecidas en la institución.

2.1.2. Realidad actual en la que se encuentra la empresa.

Rocasolida Construcciones S.A desde sus inicios se ha caracterizado como una empresa de constante crecimiento en la base a los diferentes proyectos elaborados y ejecutados en la provincia los que la han hecho ganadora de una gran credibilidad, lo cual ha conllevado al crecimiento de uno de sus activos más importantes que posee como lo es la información en cada uno de los departamentos de la organización.

Distribución Organizacional de la empresa.

Como se muestra en la figura (Fig1), tal y como se encuentra distribuida la organización de la empresa Rocasolida Construcciones S.A, en el cual se presenta la distribución funcional de la institución.

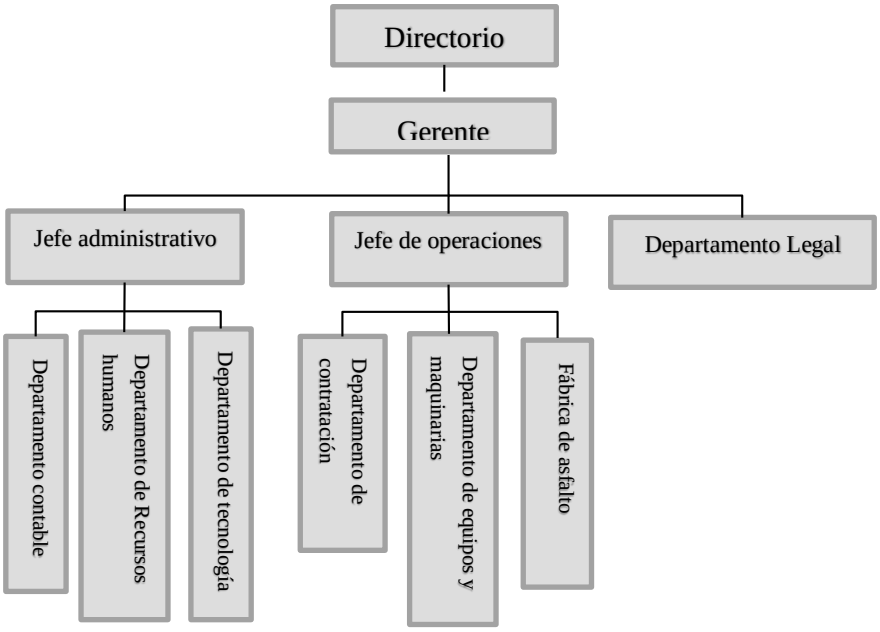

Figura 2. 1. Distribución Organizacional

A continuación se detallan los diferentes procesos que involucran la seguridad de la información en cada una de las jefaturas de la organización.

Directorio.- Los socios que representan a la empresa, el cual se reúne cada 45 días, para tratar temas relacionados a las actividades de la empresa, en relación a sus estados financieros, términos legales y el estado en el que se encuentran sus activos.

Gerente.- Legamente es el que representa a la empresa, el cual toma las decisiones que mejor le convengan a la organización

tanto en la parte administrativa y en los diferentes procesos que se desarrollan en cada uno de los departamentos con los que cuenta la institución, para la toma decisiones en la eficacia y gestión de la calidad de los procesos que cada uno de ellos conlleva.

Jefe Administrativo.- Tiene a cargo la gestión del recurso económico, el humano y tecnológico, siendo representado por un administrador en cada una de estas áreas, donde en cada una de ellas se establecen diversos procesos.

- Departamento Contable.- Es el encargado de administrar la información de los recursos económicos de la empresa, el cual cuenta con un software de contable el mismo que realiza los movimientos de ingresos, egresos, balances, proveeduría, etc.
- Departamento de Recursos Humanos.- Es el encargado de administrar la información del personal que trabaja en la empresa, el cual cuenta con un software para manejo de los sueldos de los trabajadores, dicha información se encuentra integrada con el departamento contable, para la elaboración de los roles de pago de los miembros de la organización.

- Departamento de Tecnología.- es el encargado de administrar la infraestructura de hardware y software para la gestión de los diferentes procesos que se llevan a cabo en los diferentes departamentos de la organización.

Jefe de Operaciones.- Tiene como función gestionar los diferentes servicios que brinda la empresa desde las diferentes Jefaturas que representa, a partir de la toma de decisiones de las negocios que se llevan a cabo, la gestión de proyectos de contratación con entidades públicas y privadas, y las gestión en la fabricación de asfalto de primera calidad.

- Departamento de Contratación.- Tiene a cargo el manejo de la información de las contrataciones que realiza la empresa ya sea con entidades públicas y privadas, este departamento tiene a cargo el manejo del portal de compras públicas el mismo que sube las ofertas de los proyectos que se subastan en el sector público, el mismo maneja información confidencial de los proyectos que se encuentran en ejecución y los que están por se contratados.
- Departamento de equipos y maquinarias.- Esta sección se caracteriza por manipular información que de manera integral se conecta con el departamento financiero de la

empresa, debido a las diferentes cuentas que manipula como proveeduría, egresos e ingresos entre otras.

- Fábrica de Asfalto.- Manipula los diferentes procesos que conlleva la elaboración de asfalto de primera calidad, su costo de producción y venta a las diferentes empresa públicas y privadas que demandan la adquisición de este material para el asfaltado de las vías y calles de la provincia..

Departamento Jurídico.- La información que se maneja en este departamento es en referente a las bases legales de la empresa, la contratación de trabajadores, contratos para la elaboración de obras tanto en el sector público y privado, esta sección es responsable de que en la empresa exista el análisis de las políticas, reglamentos o estatutos.

2.2. Especificar el alcance de las técnicas de seguridad de la información que se emplearan en la empresa.

La institución para establecer el alcance de las técnicas de seguridad deberá determinar el índice de aplicabilidad así como los límites según los controles a utilizar en cada uno de los procesos que se ejecutan en el Departamento de Tecnología.

Rocasolida Construcciones S.A., en lo que conlleva a su distribución organizacional cuenta con un Departamento Tecnológico, en el cual se definen como es el manejo y seguridad de la información.

Las técnicas de seguridad de la información que serán previstas en este departamento abarcan los objetivos y controles de acceso físico y lógicos, determinados en la ISO/IEC 27001, cuyo modelo establece, implementa, opera, revisa, realiza mantenimiento y se encuentra inmerso en una mejora continua, bajo este esquema es necesario recalcar que los procesos que involucran la seguridad del información en el Departamento de Tecnología tendrán una estandarización organizacional, dando como resultado un mejor tratamiento a la información que se manipula .

Basándose en la norma ISO/IEC 27001, se tomaran en cuenta para la elaboración de las técnicas de seguridad los objetivos relacionados con las políticas de seguridad, organización de la información, control de acceso, y gestión de activos físicos y lógicos. [1]

2.2.1. Seguridad de la información.

Como se establece en la cita a continuación:

“La seguridad de la información involucra técnicas que abarcan el tratamiento de la información sin dejar a un lado la

confidencialidad, integridad y disponibilidad de la misma, estas técnicas deben de ser debidamente planificadas y organizadas". [2]

Confidencialidad: "Es evitar o minimizar el acceso no autorizado y la divulgación de datos e información". [2]

Integridad: "Conlleva asegurar que los datos con los que se está trabajando son los correctos. La integridad se pone en peligro si no es bien administrada porque los datos son vulnerables o se pueden perder". [2]

Disponibilidad: "Se debe proteger los datos y evitar que se pierdan, la información a la que no se puede acceder tiene poco valor, si un contratiempo o ataque hace que se bloque el servidor principal o la base de datos, la información no estará disponible para los que la necesitan". [2]

2.2.2. Importancia de la información.

La información debe de ser protegida por lo importante y necesaria que es para la institución. En la actualidad el manejo de sistemas de información para agilizar los procesos en las organizaciones conlleva a que la información se encuentre expuesta y vulnerable ante cualquier evento que se suscite; el

poco conocimiento sobre la mitigación de riesgos ante un repentino ataque genera un impacto no favorable a la empresa lo cual puede conllevar a tener pérdidas innumerables, si su información llegase a ser alterada, lo que ocasionaría que dicha información no se llegase a preservar de una forma adecuada. [3].

Las empresas deben de ver a la información como un activo necesario e indispensable y circunstancialmente importante para la operatividad y progreso de la misma.

2.3. Aplicar los controles necesarios para implementar las Técnicas de Seguridad de la Información en la empresa.

2.3.1. Política de seguridad

"Las políticas de seguridad son el conjunto de reglas que se aplican sobre las políticas de acceso. Estas siempre son contrarias a las políticas de acceso, dado que son las encargadas de crear las excepciones de seguridad sobre la acción predefinida por la política de acceso". [4]

El Directorio de Rocasolida Construcciones aprobó la política de seguridad, basada en los controles Gestión de la Gerencia para

la seguridad de la información de la Norma ISO 27001, detallados a continuación:

Los controles utilizados para establecer las políticas en la empresa y con los cuales se va a operar utilizando así los controles de la Seguridad Física y del Entorno y control de Acceso.

El Directorio de la empresa refleja el compromiso del establecimiento de la política para la gestión de los recursos y procesos, el cual es suma importancia que se encuentren involucrados en las que se deben tomar en cada etapa de la gestión, evaluación y mejoramiento de la calidad de los procesos que se llevan a cabo en la.

El gerente de la empresa estuvo al tanto de los diferentes mejoramientos y si se da el caso la implantación de otros controles de la Norma 27001, para de esta forma alcanzar el máximo nivel de calidad necesario para lograr la certificación en la misma.

En base a las diversas observaciones legales se convierte en una necesidad que se aprueba la política, las misma que debe socializarse con todos y cada uno de los trabajadores de la empresa para que tomen conciencia de los diferentes puntos

que se establecen en la misma, la cual permite brindar servicios de calidad a los clientes de la empresa.

2.3.2. Control de Acceso

El acceso físico o lógica de los activos de una empresa en la actualidad es de suma importancia en cualquier organización sin importar cuál es el servicio que brinda, lo que conlleva a que la información que se maneja en la empresa no debe ser manipulada por usuario o trabajadores que no se encuentren debidamente autorizados para el manejo de la misma, porque que se ha comprobado por estudios realizados a nivel mundial que el manejo de la información por parte de los usuarios si no se lo lleva adecuadamente incide en el funcionamiento de los diferentes procesos que se ejecutan en la empresa.

Generalmente las políticas que se establecen en las empresas deben acatar todo lo relacionado al acceso, privilegios y restricciones que se deben cumplir para ejecución de los diferentes procesos que se realizan en la organización.

A continuación se presentan los diversos criterios que se encuentran establecidos en la Norma ISO/IEC 27001:2013, en la misma se encuentran establecido diferentes parámetros lo cuales se adoptaran para crear y establecer las políticas de

seguridad y los sub - criterios para que sean establecidos y se cumplan para que posteriormente puedan ser evaluados por cada uno de los departamentos responsables y de esta forma brindar servicios de la calidad a sus clientes.

A.9.2 Gestión de acceso al usuario

El debido control de los accesos que realizan los usuarios, ayuda a la detección de ingresos no autorizados, determinando así una organización referente a las responsabilidades que deben poseer los mismos.

A.9.2.1. Registros de usuarios

Control: El establecimiento de procesos estructurados para el registro y des-registro de los usuarios para establecer los permisos de acceso a los usuarios autorizados.

Política de Seguridad: La Jefatura de Tecnología, en quien se encarga de la distribución, asignación y registros de contraseñas que se han asignados a los jefes de los demás departamentos.

Sub - criterio:

- Establecer la unificación de usuarios, de tal forma que cada trabajador pueda acceder solamente a los recursos que se le asignaron al momento de la creación del perfil del usuario.

- Para el acceso a los diferentes recursos de la base de datos se establece una verificación del perfil del usuario para comprobar si cuenta con la respectiva autorización.

- Regular mediante un documento físico la entrega del usuario y contraseña el mismo queda bajo la responsabilidad del trabajador.

- Conservar física y lógicamente el registro formal de todas las autorizaciones efectuadas en los diferentes departamentos.

- Realizar fiscalizaciones continuas a los computadores de la institución, para de esta forma identificar si presenta alguna anomalía en el manejo por parte de los usuarios responsables de los equipos.

Responsable: Jefatura de Tecnología

A.9.2.2 Suministro de acceso a los usuarios

Control: El establecimiento formal y estructurado de un procedimiento para provisión de los accesos a los usuarios, para la asignación o revocación de los permisos de acceso a todos los tipos de usuarios y a los diferentes sistemas y servicios.

Política de Seguridad: Se establece en la política que el encargado de crear, borrar y actualizar el registro de los usuarios y cuentas es el Jefe del Departamento de Tecnología, mediante la respectiva autorización del superior al que se encuentra a cargo el trabajador.

Sub – Criterio:

- La elaboración de reportes de las cuentas que se encuentran con provisión de acceso.

- Borrar las cuentas de usuarios inactivos y de los trabajadores que no la laboran en la empresa.

- Se debe establecer por parte del Jefe del Departamento de Tecnología el procedimiento que debe llevar a cabo para la eliminación o suspensión de las cuentas de usuarios por intrusiones debidamente no autorizadas.

Responsable: Jefatura de Tecnología

A.9.2.3. Usabilidad de los Derechos de Acceso

Control: Se establecer las respectivas restricciones y controlar el uso y manejo de los accesos de los usuarios con mayor privilegio.

Política de Seguridad: Los accesos de privilegios deben estructurarse por parte de la Jefatura de tecnología quien deriva las responsabilidades a los usuarios que se categoricen con estos accesos.

Sub – criterio:

- Establecer los privilegios de acceso a los aplicativos con qué y bases de datos con la que cuenta la empresa.

- Establecer los diferentes tipos de privilegios para el acceso a la información con estableciendo la medidas de seguridad determinadas en la empresa Clasificar.

- Mediante un documento de responsabilidad firmado por el trabajador se realizara la entrega del usuario con sus respectivos privilegios por parte del Jefe del Departamento de Tecnología.

Responsable: Jefatura de Tecnología.

A.9.2.4 Procedimientos de Autenticación secreta de Usuarios

Control: Llevar un control sobre la información de la autenticación mediante un proceso de gestión formal para los usuarios que acceden a recursos que tienen un alto rango de seguridad.

Política de Seguridad: La asignación del acceso y autenticación de usuarios a recursos con un alto grado de seguridad es responsabilidad de la Jefatura de Tecnología.

Sub – Criterio:

- Enlistar las responsabilidades debidamente firmadas acerca a la autenticación establecida por parte del usuario.

- Acta de compromiso con la responsabilidad firmada de las asignaciones realizadas al trabajador.

Responsable: Jefatura de Tecnología, Usuarios responsables.

A.9.2.5. Verificación accesos.

Control: Las obligaciones de los usuarios deben de ser evaluadas frecuentemente comprobando que se estén

cumpliendo con la protección de los activos bajo su responsabilidad.

Política de Seguridad: Se deben establecer los deberes que debe de tener cada usuario en relación a los acceso que tiene cada uno de ellos.

Sub – Criterio:

- La Jefatura de Tecnología tiene la responsabilidad de realizar un reporte del monitorio de los deberes que tiene cada usuario al momento de acceder a la información de la empresa.

- Se debe de reportar al Gerente sobre las anomalías que se presentan en el acceso de los usuarios a la información a cual no tienen privilegios.

Responsable: Jefatura de Tecnología.

A.9.2.6 Retiro de Acceso.

Control: Los privilegios al acceso de la información y a las inmediaciones de la empresa por parte de los trabajadores o terceros debe de ser suspendido al momento de que ya no forme parte de misma.

Política de Seguridad: Si el trabajador deja de formar parte de la empresa o reasignado a otro puesto de trabajo se debe de informar al Departamento de Tecnología es respectivo cambio, para reajustar los respectivos procesos y los privilegios de acceso.

Sub – Criterio:

- La respectiva documentación de notificación del cambio de usuarios remitida por Gerente.

- La respectiva documentación de los cambios o retiros de los privilegios de acceso a los usuarios, debidamente registrados por parte del trabajador y el Jefe del Departamento de Tecnología.

- La respectiva documentación del cambio de rol en los privilegios del usuario al trabajador asignado por parte del Gerente.

Responsable: Jefatura de Tecnología y el Gerente

A.9.3 Responsabilidad del usuario

Para salvaguardar la autenticación de la información es necesario socializar a los usuarios la importancia de la

información que manipulan, para concientizar la seguridad de la información y la responsabilidad que con la que debe procesar la misma.

A.9.3.1 Autenticación de la información

Control: La información secreta debe de ser autenticada, es así que se debe de capacitar a los usuarios que asumirán las responsabilidades de estas autenticaciones.

Política de Seguridad: El manejo de la autenticación de claves secretas está bajo la responsabilidad juramentada de tal forma que se personalice el manejo de cómo se encuentren establecidas.

Sub – Criterio:

- El respectivo documento que ampare la asignación de los privilegios al usuario de parte de la Jefatura de Tecnología.

Responsable: Jefatura de Tecnología, Usuario.

A.9.4 Accesos no autorizados a sistemas y aplicaciones.

Controlar los accesos sin la respectiva autorización a los sistemas y aplicaciones con que cuenta la empresa.

A.9.4.1 Restricciones de acceso

Control: Los sistemas y aplicaciones deben de contemplar las debidas restricciones de acceso. Estas restricciones deben de establecerse en las políticas de seguridad.

Política de Seguridad: La Jefatura emitirá el respectivo informe de los accesos realizados sin el debido permiso establecido en las restricciones, mediante un monitoreo continuo de los accesos no autorizados que fueron realizados por usuarios sin debidos privilegios.

Sub – Criterio:

- Reportes de parte del Jefe del Departamento de Tecnología.

- Accesos sin la respectiva autorización, realizar medidas preventivas.

Responsables: Jefatura de Tecnología, Usuarios.

2.3.3. Gestión de los activos

A lo interna de la empresa se deben establecer las diferentes responsabilidades que le corresponden a los usuarios en lo que conlleva al manejo y la utilización de los activos, los que deben de encontrase determinados desde su utilidad y las

especificaciones que representan cada uno de ellos, de esta forma llegar a tener un manejo oportuno y de responsabilidad de cada uno de los trabajadores de la empresa.

Para establecer un mejor estudio de los criterios que se encontraran incluidos en el control de los activos de la empresa tanto lógicos (software) o físicos (hardware) los cuales se los ha dividido para establecer un mejor criterio.

A continuación se presenta una descripción del inventario de la estructura de los activos físicos y lógicos con los que cuenta la empresa.

Inventario de los equipos físicos (hardware).

1. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB .
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la Responsabilidad de la recepción.

2. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la Responsabilidad del directorio.

3. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del Jefe del Departamento.

4. Tres computadores de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.

- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del jefe del Departamento.

5. Dos computadores de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del Jefe departamental .

6. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 20 de enero del 2014.

- Bajo la responsabilidad del jefe Jurídico.

7. Un computador de escritorio Hp con las siguientes características

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 20 de Marzo del 2014.
- Bajo la responsabilidad del Gerente.

8. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del jefe administrativo.

9. Dos computadores de escritorio Hp con las siguientes características:

- Series HP 21-2035T.

- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del Departamento de maquinarias.

10. Tres computadores de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 20 de marzo del 2014.
- Bajo la responsabilidad del jefe departamental y dos técnicos.

11. Un computador de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.

- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 30 de enero del 2014.
- Bajo la responsabilidad del jefe de la fábrica de asfalto.

12. Dos computadores de escritorio Hp con las siguientes características:

- Series HP 21-2035T.
- Intel Core i3-4150T 3.0GHz.
- 8GB de memoria RAM.
- Capacidad de almacenamiento de 1.000GB.
- Windows 8 (no cuenta con licencia).
- Adquirido el 20 de marzo del 2014.
- Bajo la responsabilidad del Jefe de Tecnología y el técnico operativo.

13. Un servidor Hp con las siguientes características:

- HP ProLiant Gen8.
- Con Procesador E3-1220 v3 (4 núcleos, 3,1 GHz, 8 MB, 80 W) Intel ® Xeon ®.
- 16 GB de memoria RAM.
- Capacidad de almacenamiento de 4TB.
- Microsoft Windows Server 2012.
- Adquirido el 25 de abril del 2013.

- Bajo la responsabilidad de la Jefatura Tecnológica.

Inventario de Activos lógicos de la Empresa (Software)

1. **Sistema operativo :** Windows 8.1

   Detalle: Para la operatividad del computador consta del sistema operativo Windows, cabe indicar que la Empresa no posee las respectivas licencias.

   Usabilidad: Quien se encarga de la funcionalidad y operatividad de las aplicaciones es el Sistema Operativo por eso es de mucha importancia este requisito lógico.

   Beneficiario: En su totalidad la empresa cuenta con 16 computadoras, las mismas que portan el Windows 8.

   Lugar: Departamentos y jefaturas que conforman la empresa.

   Declaración de responsabilidad: Los diferentes trabajadores que realizan funciones en cada uno de los Departamentos y jefaturas.

2. **Utilitarios de oficina:** Microsoft Office 2013

   Detalle: Para las diversas tareas ofimáticas que se realizan en los Departamentos de la Empresa, no presenta licencias.

Usabilidad: Para la ejecución y funcionalidad de las tareas de oficina en cada uno de los departamentos, facilita las determinadas necesidades de procesamiento de texto, hojas de cálculos, presentaciones, etc.

Beneficiario: En su totalidad la empresa cuenta con 16 computadoras, las mismas que portan este utilitario.

Lugar: Departamentos y jefaturas que conforman la empresa.

Declaración de responsabilidad: Los diferentes trabajadores que realizan funciones en cada uno de los Departamentos y jefaturas.

3. **Software Contable:** Génesis.

   Detalle: El usos de este software se lo realiza para la generación de balances, roles de pagos, control de activos, proveeduría, entre otros.

   Usabilidad: Es de suma utilidad para la empresa la cual permite realizar los balances financieros de las diferentes actividades realizada por la organización.

   Beneficiario: El software contable lo poseen del Departamento Contable, la fábrica de asfalto y el departamento de maquinaria y equipos.

Lugar: Departamento Contable, la fábrica de asfalto, y el Departamento de maquinaria y equipos.

Declaración de responsabilidad: Los trabajadores que laboran en cada uno de los departamentos.

4. **Herramienta para Diseños de Construcción:** Auto CAD 2013

   Detalle: Este tipo de software se lo utiliza en la ingeniería para el diseño de planos estructurales para las diferentes obras que se encuentran en desarrollo y para las que se encuentran por contratar.

   Usabilidad: Es de suma importancia para la empresa la cual es utilizada para el desarrollo de los diseños arquitectónicos e infraestructura de la construcción.

   Beneficiario: Dicha herramienta es utilizad por varios equipos del departamento de contratación.

   Lugar: Departamento de Contratación

   Declaración de responsabilidad: Los trabajadores del Departamento de contratación.

5. **Herramienta para la elaboración de presupuestos en la construcción:** Análisis de Precio Unitario

Detalle: Este software le permite el análisis de los costos de producción en la construcción.

Beneficiarios: Este software es de suma utilidad para el cálculo en las contrataciones referentes a los presupuestos de mano de obra, costo, entre otros.

Usabilidad: Este software es manipulado por los asistentes de contratación que laboran en el Departamento de Contratación.

Lugar: Área de Contratación

Declaración de responsabilidad: Asistentes que laboran en el Departamento de Contratación.

6. **Sistema Operativo para servidores:** Windows Server 2012.

   Detalle: Es un Sistema operativo desarrollado para servidores.

   Beneficiarios: Este sistema operativo es de suma importancia para la empresa, en el cual se encuentra alojada la Base de Daros de la organización.

   Servidor: Se encuentra instalado en el Área de Tecnología.

Lugar: Área de Tecnología

Declaración de responsabilidad: Jefatura de tecnología.

7. **Gestor de Base de Datos:** Mysql.

   Detalle: El Sistema de Gestión de Base de Datos mysql Worbrench permite realizar el modelado de la base de datos y su administración.

   Usabilidad: Es de suma utilidad debido a que la base de datos contiene almacenada toda la información de la empresa.

   Beneficiario: Se encuentra instalada en el servidor alojado en la jefatura de tecnología.

   Lugar: Jefatura de Tecnología

   Declaración de responsabilidad: Jefatura de tecnología.

CAPÍTULO 3

ANALISIS DE RESULTADOS

3.1. Evaluar la usabilidad y la aplicabilidad de los controles aplicados en la implementación de las técnicas de seguridad.

Uno de los mecanismo que se utilizados para evaluar el estado actual de la operatividad de los diferentes procesos que se llevan a cabo en una empresa u organización.

La auditoría que se realizó al Departamento de Tecnología de la empresa Rocasolida Construcciones S.A., en la misma se pudo constatar el funcionamiento de las técnicas de la seguridad de la Información, teniendo en cuenta que los parámetros evaluados

establecen los diferentes factores del cómo se procesando la información en el Departamento.

3.1.1. Metodología de la valoración de riesgos.

En el estudio del manejo de la información por parte de la Empresa, se estableció una clasificación de los recursos de la información que manipula la organización la misma que se clasifico en base a la disponibilidad, confidencialidad e integridad de este activo que uno de los más importantes dentro de una Organización.

En la Norma ISO/IEC 27001:2013, establece los controles de la seguridad de la información los cuales se consideran para la realización de la auditoria interna para de esta forma instaurar una evaluación de los mecanismos y funciones de la utilización que se está llevando a cabo.

Confidencialidad: "Certifica que la información sea procesada de una forma segura y que sea accesible para quien sea autorizado". [5]

Tabla 1. Diseño de los criterios de evaluación de la confidencialidad de la información.

Criterio	Descripción
0	Manipulación de la información que no es necesario que se restringa su usabilidad para los empleados.
1	La información que manipula los trabajadores de la empresa y que tiene que ser de carácter público no ocasione ni ponga en peligro los bienes de la Empresa.
2	Clasificación de la información que será manipulada por un grupo exclusivo que si se publica llegaría a perjudicar poniendo en peligro los bienes de la Empresa.
3	El establecimiento de la información para los usuarios en la empresa como el gerente, directorio y jefes departamentales

Integridad: "La información a más de ser confiable debe de ser segura es así que la integridad refleja esta característica"**.** [5]

Tabla 2 Diseño de los criterios de evaluación de la integridad de la información

Criterio	Descripción
0	La variación y Administración sin la debida autorización, para una recuperación ágil, la cual no altere la funcionalidad de la empresa.
1	La variación y Administración sin la debida autorización, con una recuperación ágil, lo cual conllevaría a un alto grado de riesgo de la funcionalidad de la empresa.
2	La variación y Administración sin la debida autorización, con una recuperación ágil, lo cual conlleva a un alto grado de riesgo en desventajas de la funcionalidad de la empresa.
3	La variación y Administración sin la debida autorización, con un alto grado de complicación y recuperación, lo cual conlleva a altos riesgos en desventajas de la funcionalidad de la empresa.

Disponibilidad: “Esta propiedad refleja la accesibilidad de la información en una entidad con los privilegios respectivos”. [5]

Tabla 3. Diseño de los criterios de evaluación de la disponibilidad de la información

Criterio	Descripción
0	El no tener acceso no daña la funcionalidad de las tareas de la empresa
1	El no tener acceso continuo durante algunos días, conllevaría a grandes desventajas a la empresa.
2	El no tener acceso continuo crecidamente de 10 horas, conllevaría a grandes desventajas a la empresa.
3	El no tener acceso continuo crecidamente de 30 minutos, conllevaría a grandes desventajas a la empresa.

Para la elaboración de la auditoria se enfocó en los criterios de evaluación de alto, medio y bajo, relacionados con la confidencialidad, la integridad y la disponibilidad de la información, de tal forma poder establecer la diferentes amenazas y vulnerabilidades que se muestran. A continuación se muestran las diferentes concepciones basadas en los criterios establecidos con anterioridad:

Análisis de riesgo: La manipulación automatizada de la información estima los riesgos mediante la identificación de las fuentes. [5]

Valoración del riesgo: La evaluación de riesgos se establece en análisis global en los procesos que se realiza con la información. [5]

Tabla 4. Índices de tasación para valorar los riesgos.

Recursos físicos y lógicos	**Estimación**			
	C	**I**	**D**	**Total**
Base de Datos	1	1	1	1

PC	1	1	1	1
S.O	1	1	1	1
Programa	1	1	1	1

Tabla 5. Criterios de valoración de riesgos.

Amenazas	**Recurrencia**	**Vulnerabilidad**	**Riesgo**
- Hackers	1	Actualización de los parches del sistema operativo	1
- Virus	1	No existe la respectiva actualización del software antivirus	1
	1	El ingreso a área de	1

- Seguridad física		servidores no cuenta con la debida seguridad.	
- Virus - Marlware - Acceso al sistema - Seguridad	1 1 1	No se cuenta con la licencia del software antivirus Poca socialización a los usuarios sobres los diferentes métodos de ataque Poca socialización a los usuarios sobre el manejo de contraseñas y sus sesiones	3 1 2

Física	2	Poca socialización a los usuarios sobre el manejo del lugar de trabajo donde desenvuelve	2
- Seguridad lógica	1	No se cuenta con las respectivas licencias del sistema operativo.	1

C: Confidencialidad **Alta: 1**

I: Integridad **Media: 2**

D: Disponibilidad **Baja: 3**

3.2. Gestión de la Seguridad de la Información y mejora.

Instaurar las mejoras necesarias a establecer en la empresa con los criterios que se presentan a continuación:

- El Jefe del Departamento Tecnológico es el principal comprometido en las diferentes vulnerabilidades halladas en lo que corresponde a los activos de software relacionados más a un al sistema operativo con que cada una de las computadoras de la empresa debido a que las mismas no cuenta con las respectivas

licencias del registro del sistema operativos, lo que representa un gran riesgo para la información de la empresa, cual se encuentra vulnerable ante un posible ataque ya sea desde el exterior o el interior de la empresa, se deben realizar un reporte del alcance puede tener esta eventual amenaza a Gerente para que se tomen las respectiva medidas ante este suceso y se reestructure el software para que garantice la seguridad de la información.

- La obligatoriedad de que el gerente revise los respectivos informes realizados por el Jefe del Departamento Técnico, de tal manera que se pueda evidenciar el cumplimiento de los procesos y procedimientos que se encuentran debidamente normalizados.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En la actualidad la información es uno de los activos más importantes de una empresa, desde mi punto de vista todas organizaciones e instituciones deben de privilegiar el aseguramiento de este activo, es primordial para el funcionamiento y operatividad de la empresa, con este antecedente se puede instaurar la norma para la mejora en los procesos y administración de la información.

2. En el empleo de la norma en el Departamento Tecnológico, se pudo detectar que determinados procedimiento no se realizaban de una

manera ordenada con una estructura organizativa, mejorando así la operatividad en los procesos de la empresa.

3. Rocasolida Construcciones S.A., con pocos de años de creación institucional maneja una gran cantidad de procesos los cuales son de mucha importancia para la empresas, dicha información siempre tiene que encontrarse disponible, al realizar la auditoria interna se pudo evaluar que existen ocasiones en que por tener esta disponibilidad, es dejado de la lado la integridad de la misma.

RECOMENDACIONES

1. Se debe de tener el respectivo respaldo de las autoridades de la institución para los nuevos procesos de cambio, para que de esta forma se logre ejecutar las diferentes fases de los cambios en la organización.

2. El apoyo del gerente es fundamental, ya que es el responsable inmediato ante las decisiones que se tomen, ante la aplicación de la norma es necesario explicar de forma clara y concisa el alcance que va a tener y el respectivo acompañamiento con él debe de contar.

3. Se debe de mantener continuamente bien informado tanto al Directorio como al Gerente de los diferentes eventos o controles que se estiman

implantar, para que de esta forma el Gerente se encuentre bien informado de las respectivas acciones tomadas.

4. En el Departamento de Tecnología de la Empresa Rocasolida Construcciones S.A, se estableció en conjunto con el Directorio y el Gerente acogerse a un proceso de mejora continua, para en un futuro acreditar en los diferentes controles de la NORMA ISO/IEC 27001:2013, desde mi punto de vista le recomiendo no desmayar ante la posibilidad de la variación en los aspectos de la seguridad de cómo se encontraban antes y de cómo se encuentran ahora.

BIBLIOGRAFÍA

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

[2] J. I. Luca de Tena, CompTIA Security+ Study Guide, Fifth Edition ed., Madrid: Grupo Anaya, S.A., 2011, pp. 41- 42.

[3] C. Álvarez, "La ley y la seguridad de la información una perspectiva regional," *Sistemas Rastreando la Inseguridad,* vol. 1, no. 101, pp. 12-20, Abril 2007.

[4] M. Jimeno, C. Maria, C. Miguez, A. Matas and E. Heredia, La biblia del Hacker, Madrid: Grupo Amaya S.A., 2012.

[5] K. Astudillo, Hacking Ético 101, Segunda ed., Guayaquil, Guayas: Lexington, 2013, pp. 268-269.