DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMA DE LA EMPRESA RYMCO S.A BAJO LA NORMA ISO IEC/27001:2013

PEDRO ANTONIO SAMPER IBÁÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2015

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMA DE LA EMPRESA RYMCO S.A BAJO LA NORMA ISO IEC/27001:2013

PEDRO ANTONIO SAMPER IBÁÑEZ

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2015

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Barranquilla, 31 de mayo de 2015

AGRADECIMIENTOS

Agradecemos a los docentes y la Universidad Nacional Abierta y a Distancia UNAD por la transferencia del conocimiento que nos permitió adaptar varias herramientas vistas durante la especialización de Seguridad informática y proponer esta guía metodología, herramienta que son factor importante en el desarrollo de la implementación de un sistema de gestión de la seguridad informática SGSI.

A los tutores de la especialidad por su acompañamiento y retroalimentación en el proceso de elaboración de esta guía metodológica.

A los compañeros de la especialidad en el desarrollados de cada uno de los cursos terminados por sus aporte individual y grupal que permitió consolidar los diferentes conocimientos adquirido en cuanto a la seguridad informática.

TABLA DE CONTEIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTAS DE ANEXOS

Pág.

GLOSARIO

A

ACCIÓN CORRECTIVA: acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

ACCIÓN PREVENTIVA: medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

ACEPTACIÓN DEL RIESGO: decisión informada de asumir un riesgo concreto.

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ALCANCE: ámbito de la organización que queda sometido al SGSI.

AMENAZA: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

ANÁLISIS DE RIESGOS CUALITATIVO: análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

ANÁLISIS DE RIESGOS CUANTITATIVO análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

.

AUDITORÍA: proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

AUTENTICACIÓN: provisión de una garantía de que una característica afirmada por una entidad es correcta.

AUTENTICIDAD: propiedad de que una entidad es lo que afirma ser.

.

C

COMPROMISO DE LA DIRECCIÓN: lineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización,

revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

CONFIDENCIALIDAD: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

.

CONTROL: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CONTROL CORRECTIVO: control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL DETECTIVE: control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

CONTROL PREVENTIVO: control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

CORRECCIÓN: acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

D

DECLARACIÓN DE APLICABILIDAD: documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

.

DIRECTIVA O DIRECTRIZ: una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

E

ESTIMACIÓN DE RIESGOS: proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud sonaceptables o tolerables.

EVALUACIÓN DE RIESGOS: proceso global de identificación, análisis y estimación de riesgos.

F

FASE 1 DE AUDITORÍA: etapa de la auditoría de primera certificación en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.

FASE 2 DE AUDITORÍA: etapa de la auditoría de primera certificación en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo eficaz.

G

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información

GESTIÓN DE RIESGOS: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I

IDENTIFICACIÓN DE RIESGOS: proceso de encontrar, reconocer y describir riesgos.

IEC: organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

IMPACTO: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud.

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO/IEC 27001: norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002: código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ISO 9001: norma que establece los requisitos para un sistema de gestión de la calidad.

N

NO CONFORMIDAD: de un requisito.

NO REPUDIO: según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

O

OBJETIVO: declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

P

PDCA: plan-do-check-act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

PLAN DE TRATAMIENTO DE RIESGOS: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

PROCESO: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

PROPIETARIO DEL RIESGO: persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

R

RECURSOS DE TRATAMIENTO DE INFORMACIÓN: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO RESIDUAL: el riesgo que permanece tras el tratamiento del riesgo.

S

SALVAGUARDA: realizar una copia de información.
SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información.

SELECCIÓN DE CONTROLES: proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: sistema de Gestión de la Seguridad de la Información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

T

TRATAMIENTO DE RIESGOS: proceso de modificar el riesgo, mediante la implementación de controles.

TRAZABILIDAD: según [CESID: 1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

V

VULNERABILIDAD: debilidad de un activo o control que puede ser explotada por una o más amenazas.

R E S U M E N

Hoy en día nos encontramos que en algunas empresas en Colombia sus profesionales del área de informática, aún se encuentran llenos de tabúes, en cuanto a la protección de la información. Considerando que con el solo hecho de tener software y antivirus licenciados y de realizar periódicamente backup es suficiente para estar protegidos ante posibles ataques informáticos. Es decir aun no admiten la necesidad de implementar los Sistemas de Gestión de la Seguridad de la Información SGSI. Este proyecto es un diseño metodológico para implementación de un SGSI en el área de sistema de la empresa RYMCO S.A bajo la norma ISO IEC/27001:2013.

- ✓ Diseño de un Sistema de Gestión de la Seguridad de la Información.
- ✓ Área de Sistema de la empresa RYMCO S.A.
- ✓ Norma ISO IEC/27001:2013.
- ✓ Metodología del Diseño.
- ✓ Garantizar la protección de los recursos.

Palabras claves

DISEÑO, MODELO, ISO 27001: 2013, NORMAS, CONTROLES, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, DISPONIBILIDAD, INTEGRIDAD DE LOS DATOS, CONFIDENCIALIDAD DE LA INFORMACIÓN, VULNERBILIDAD, RIESGOS Y AMENAZAS.

INTRODUCCION

La cantidad y complejidad de información y de los sistemas informáticos sigue teniendo un aumento considerable día a día, por lo cual las organizaciones se enfrentan a retos inimaginables para poder abordar, las amenazas que persisten en la actualidad y que representan riesgos críticos para la seguridad de cualquier entidad.

Toda empresa necesita proteger sus activos que son lo más valioso "la información", es por ello que la empresa requiere establecer una disciplina de seguridad con el fin de asegurar y controlar sus procesos de negocio y por ende su participación operativa en mercado.

En el desarrollo de este trabajo se analizarán los riesgos del área de sistema, se realizarán las recomendaciones pertinentes para mitigar los riesgos, se establecerán políticas en cuanto al empleo y uso de software y hardware computacional y redes, para que sus empleados puedan abordar buenas prácticas de seguridad de la información se recomendara un plan de continuidad para el área de sistemas y se darán unas directrices para la implementación del sistema de gestión de la seguridad de la información.

1 DESCRIPCIÓN DEL PROBLEMA

La seguridad informática ha adquirido una gran importancia en los tiempos más recientes, sobre todo en las organizaciones y los miembros que conforman. Esta situación se debe a que cada día las amenazas informáticas, el acceso indebido a los sistemas informáticos, a la información, los programas maliciosos, ataques informáticos y fallas de los servicios y sistemas, representan un problema que podría generar efectos catastróficos.

En la empresa RYMCO S.A se presentan fallas en la manipulación de los equipos hardware y software por parte de los empleados de la organización, existente unas normas sobre el manejo de equipos y software en el departamento de sistema, pero no se ejerce un adecuado control hacia los usuarios o personal de la empresa entre las cuales tenemos:

- ✓ Se comparte contraseña entre los empleados
- ✓ Daños en los equipos informáticos no reportados
- ✓ Equipos de cómputos obsoletos que requieren ser reemplazados
- ✓ Las contraseñas generadas por los usuarios son muy débiles
- ✓ Traslado de equipos de cómputos de una sección a otra sin autorización
- ✓ Las actualizaciones de los equipos de cómputo no se cumplen los cronogramas preestablecidos siendo un factor primordial que afecta en la disponibilidad de los recursos de hardware y software
- ✓ Los daños del cableado estructurado no son atendidos de la mejor forma
- ✓ No existen políticas de seguridad para el control de instalación de software

1.1 HIPÓTESIS

El diseño de implementación de un SGSI en el área de sistema de la empresa RYMCO S.A, lograra la protección adecuada de sus activos e información, mediante la implementación de las directrices de la norma ISO IEC/27001:2013.

2 FORMULACIÓN DEL PROBLEMA

Debido a los problemas presentados y las fallas de seguridad evidenciadas, como también el poco conocimiento que tiene la empresa en cuanto a la seguridad de la información se puede preguntar:

¿Cómo se puede mitigar los riesgos[1] del área de sistemas de la empresa RYMCO S.A y proponer recomendaciones de seguridad de la información que protejan los activos informáticos y concienticen al personal de la organización?

1 Mitigar los riesgos Son medidas tomadas con anticipación al desastre, con el ánimo de reducir o eliminar su impacto sobre la sociedad y Medio Ambiente.

3 JUSTIFICACIÓN

Un SGSI2 es, tal como su nombre lo indica, un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Toda organización tiene objetivos, por lo general relacionados con el mercado y los negocios, y requiere que desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable. Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, y aquí entra en juego un SGSI.

El SGSI debe ser considerado a la hora de administrar la seguridad en una organización como un todo que garantice la seguridad de los activos, por tanto el desarrollo de este proyecto beneficiara a la empresa RYMCO S.A en lo siguiente:

- ✓ Que el área de sistema se establezca como un departamento solido en beneficio de la empresa
- ✓ El diseño del sistema de seguridad información en el área de sistemas, sirva como guía para se implemente en toda la organización
- ✓ Los riesgos, las amenazas, y las vulnerabilidades sean conocidos y mitigados y no generen un impacto con pérdidas representadas en dineros
- ✓ Mantener la integridad, confiabilidad, y disponibilidad de la información esencial para alcanzar los objetivos del negocio

2 ***SGSI*** *Sistema de gestión de la seguridad de la información.*

4 OBJETIVOS

4.1 *OBJETIVOS GENERAL*

Diseñar un sistema de gestión de la información (SGSI), para el área de sistemas de la empresa RYMCO S.A. bajo la norma ISO IEC/27001:2013

4.2 *OBJETIVOS ESPECÍFICO*

- ✓ Mitigar el riesgo en el área de sistemas que puedan causar perjuicios a la empresa.
- ✓ Fomentar la incorporación de las políticas de seguridad en el área de sistemas y que se pueda extender a otras áreas.
- ✓ Garantizar la protección de los recursos software y hardware.
- ✓ Establecer un plan de contingencia para el área de sistema de la empresa.
- ✓ Proponer herramientas que faciliten el diseño del SGSI mediante la norma ISO/IEC 27001:2013 en cada una de sus etapas.

5 MARCO REFERENCIAL

5.1 *ANTECEDENTES*

La finalidad de este proyecto es recomendar la necesidad futura de implementar en área de sistemas de le empresa RYMCO S.A un SGSI bajo la norma ISO IEC/27001:2013.

En Octubre de 2014 es presentado el proyecto de diseño de un SGSI en el área de sistemas de la empresa RYMCO S.A bajo la norma ISO IEC/27001:2013 en la Facultad de Ingeniería de sistema posgrado de la Especialización de Seguridad Informática de la UNAD[3], como requisito para optar el Titulo Especialista en Seguridad Informática.

Mediante la investigación realizada se diseñara un SGSI, que busca establecer unas guías, directrices, que permita mejorar los controles y establecimiento de políticas para salvaguardar los activos de la empresa.

Dentro de las experiencias más radicales presentadas en la empresa en donde se evidencia los accesos no autorizados por el personal de la empresa dentro de la red poniendo en peligro la información son unas de las razones de la realización de este proyecto.

5.2 *MARCO LEGAL*

Partiendo de la ley emanada del congreso de la república Ley N°1273 del 5 de enero de 2009, por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

DECRETA:

Artículo 1°. Adicionase el código Penal con el Titulo VII BIS denominado "Dela protección de la información y de los datos" del siguiente tenor:

---

3 *UNAD. Universidad Nacional Abierta y a Distancia.*

5.2.1 **Capitulo Primero.** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

ARTICULO 269A Acceso abusivo a un sistema informático. El que sin autorización o por fuera de lo acordado, acceda a todo o parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigente.

ARTICULO 269B Obstaculización ilegitima de sistema informático o red de telecomunicaciones. El que sin estar facultado para ello, impida u obstaculice el funcionamiento o acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTICULO 269C. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTICULO 269D: Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses en multa de mil (100) a mil (1000) salarios mínimos legales mensuales vigentes.

ARTICULO 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envié, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

ARTICULO 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envié, compre, intercepte, modifique, o emplee códigos personales, datos, personales contenidos en ficheros, archivos, bases de datos o medios semejantes incurrirá en pena de prisión de cuarenta y ocho (48) a no venta

y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

ARTICULO 269G: Suplantación de sitios web para capturar datos personales. El que, con objeto ilícito, sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute programe o envié páginas electrónicas, enlaces o ventas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

ARTICULO 269H: Circunstancia de agravación punitiva

Las penas imponibles de acuerdo con los artículos descriptos en este título, se aumentaran de la mitad a tres cuarta partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero nacional o extranjeros
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información.
4. Revelando o dando a conocer el contenido de la información
5. Obteniendo provecho para sí o para terceros
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional
7. Utilizando como instrumento a un tercero de buena fe
8. Si quien incurra en esta conducta es el responsable de la administración o manejo y control de la información

5.2.2 **Capitulo Segundo.** De los atentados informáticos y otras infracciones.

ARTICULO 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informática, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación establecidos, incurrirá en la pena señaladas en el artículo 240 de este código.

ARTICULO 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con penas más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte

(120) meses y en multa de doscientos (200) a mil quinientos (1500) salarios mínimos legales mensuales vigentes.

5.3 MARCO TEÓRICO

5.3.1 **SGSI.** El concepto El concepto de un SGSI es el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de la información minimizando a la vez los riesgos de la seguridad de la información.4

Como todo proceso de gestión de un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los entornos externos.

Beneficios:

1. Un análisis de riesgo, identificando amenazas, vulnerabilidades e impacto de las actividades empresariales
2. Una mejora continua a la gestión de la seguridad
3. Una garantía de continuidad y disponibilidad del negocio
4. Reducción de los costos vinculados a los incidentes
5. Incremento de los niveles de confianza de los clientes
6. Aumento del valor del valor comercial yo mejora de la imagen de la organización
7. Voluntad de cumplir con la legislación vigente

Actualmente nos encontramos en la era de la información y el conocimiento, las organizaciones deben tener como uno de sus principales objetivos el cuidado, seguridad y disponibilidad de sus activos de información: sin la adecuada preservación de la información de una empresa como el caso de RYMCO S.A, esta perderá aquellas ventajas que le hacen ser competitivas y terminara por desaparecer del mercado; dado que entre más tecnología y reconocimiento en las organizaciones mayor es el riesgo de la información si no existe protección contra amenazas y vulnerabilidades.

Para una adecuada gestión de la información es necesario diseñar una metodología rigurosa y clara, que con base en normas preestablecidas le permiten a cualquier individuo de la organización asegurar la disponibilidad y seguridad de la información.

4 Fuentes. https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

5.3.2 **Norma ISO 27001-2013.** La International Organización de Estandarización-ISO e International Electrotécnica Comisión – IEC, desarrollaron la familia de Normas ISO/IEC 27000, donde se proporcionan los lineamientos para la gestión de la seguridad en la información en cualquier empresa; para efecto de este trabajo nos enfocaremos en las normas ISO 27001 – 27002.[5]

ISO es la única norma internacional auditable que define los requisitos para un SGSI. La norma se ha concedido para garantizar la selección de controles de la seguridad adecuada y proporcional.

Ello ayuda a proteger los activos de la información y otorga confianza a cualquier parte interesada, sobre todo a los clientes. La norma adopta un enfoque por proceso para establecer, implementar, operar, supervisar, revisar y mantener y mantener un SGSI.

5.4 *SEGURIDAD DE LA INFORMACIÓN*

El termino Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; Sin embargo entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.6
La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra el diseño de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que

5 Fuentes. http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

6 Fuentes. http://190.90.112.209/http/criptografia/Seguridad_de_la_informacion.pdf

surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.[7]

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial.8 La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

La integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La seguridad de la información se encarga de protegerla de una amplia gama de amenazas, a fin de garantizar la continuidad comercial del negocio, minimizar los daños y maximizar el retorno sobre las inversiones y las oportunidades,

7 Fuentes. http://190.90.112.209/http/criptografia/Seguridad_de_la_informacion.pdf

8 Fuentes. http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

normalmente se logra desarrollando un conjunto adecuado de controles que abarcan políticas y procedimientos, involucrando recursos humanos, hardware y software9. Es decir, el término seguridad de la información cubre un amplio espectro de actividades, y parte de nuestro trabajo como profesionales de la seguridad, será hacer recomendaciones y tomar acciones para minimizar los riesgos y exposición de la información y demás activos. Estas actividades, muchas veces no son sencillas, pero deberemos realizarlas correctamente para tener una chance de mantener la seguridad de la información de la empresa dentro de niveles razonables.

La información representa valor para las organizaciones; por lo tanto es un activo ya que es un conjunto de datos, es esencial para el negocio de una organización, y en consecuencia es necesario asegurar su protección.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de la inversión y las oportunidades comerciales.

5.4.1 **Los Activos.** Cada organización tiene activos y recursos valiosos. La identificación de activos es el promedio del cual una compañía intenta valuar la información y sus sistemas. En algún caso simple como contabilizar las licencias de software; estas valuaciones de activos físicos son un proceso de contabilización normal que una empresa debería realizar en forma rutinaria, más dificultosa el proceso de identificación de activos es intentar asignarle un valor a la información. En algunos casos, podría ayudarnos si intentamos determinar qué sucedería en caso que nuestra información se pierda o se vuelva no disponible. Si la ausencia de esta información provocaría que el negocio se detenga, esta información es muy valiosa y se podrá valuar según el costo provoque a la empresa esta detención.

Los activos de la información de las organizaciones enfrentan amenazas de seguridad entre ellas: fraudes por internet, computador, espionaje, sabotaje, hurto, fenómenos naturales, fuego o inundaciones. Las causas de daño como códigos maliciosos, spam, o hackers se hacen cada vez más comunes, más efectivas, más ambiciosas y cada vez más sofisticadas10

9 Fuentes. https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdf

10 Fuentes. http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

5.5 MARCO CONTEXTUAL

5.5.1 **Historia de la Empresa**. RYMCO S.A. establecida en el año 1980, nace como una sociedad limitada RYMCO Ltda. Es una empresa administrada profesionalmente, cuyo objeto social es producir y comercializar artículos médicos estériles para usar una sola vez.

En el año de 1980 empieza la producción inicial de jeringas y agujas y es así como se fabrican las jeringas de 2 ml y 5 ml de dos piezas con sus respectivas agujas, las cuales sustituirían las jeringas que en ese momento se importaban. Esta primera etapa tuvo muchos tropiezos como consecuencia del desconocimiento del mercado y por la resistencia al cambio que ofrecían los clientes que utilizaban las jeringas importadas y además los que en ese momento utilizaban las jeringas de vidrio.

Desde entonces, la empresa ha crecido ampliando su capacidad instalada, así como también la diversidad de sus productos, fabricando equipos para infusión tales como equipos peri craneal[11], equipos para venoclisis[12], equipos de transfusión de sangre[13], catéter[14], buretas y adaptador para terapia intermitente.

La empresa inicialmente se orientó hacia el mercado nacional, pero poco a poco fue incursionando en el mercado internacional y ha atendido satisfactoriamente a clientes en el mercado de centro y sur América con gran éxito.

Para lograr esto RYMCO S.A. ha mantenido un proceso de mejoramiento de la calidad de sus productos, así como también de orientar las características de los mismos hacia el cumplimiento de las exigencias mundiales.

RYMCO S.A. es la empresa más grande del país en la producción de jeringas.

---

[11] *Equipo Pericraneal. Es una aguja de infusión intravenosa con aletas que aseguran la venopuntura cuando se fijan a la piel.*

[12] *Equipo para Venoclisis. Es un dispositivo destinado a ingresar por vía intravenosa, ya sea periférica o central, la infusión continua de fluidos. Está disponible en 2 presentaciones Macrogotero y Microgotero.*

[13] *Equipo de Transfusión de Sangre. Utilizado para la administración o transfusión de sangre, sus hemocomponentes y/o sus derivados, con el fin de recuperar el volumen sanguíneo*

[14] *Catéter venoso central. Un catéter venoso central es una cánula que se inserta quirúrgicamente que permite a los médicos administrar medicamentos y otros líquidos por vía intravenosa (IV), además de extraer sangre.*

Actualmente realiza exportaciones principalmente a países tales como:

Brasil, Argentina, Ecuador, Chile, Venezuela, Bolivia, Salvador, Perú.

Sus instalaciones físicas están ubicadas en Barranquilla Colombia Dirección: Calle 80 # 78 B 51.

5.5.2 **Misión.** RYMCO S.A produce y comercializa dispositivos médicos de óptima calidad buscando contribuir al mejoramiento de la salud de sus usuarios y la constante satisfacción de nuestros clientes.

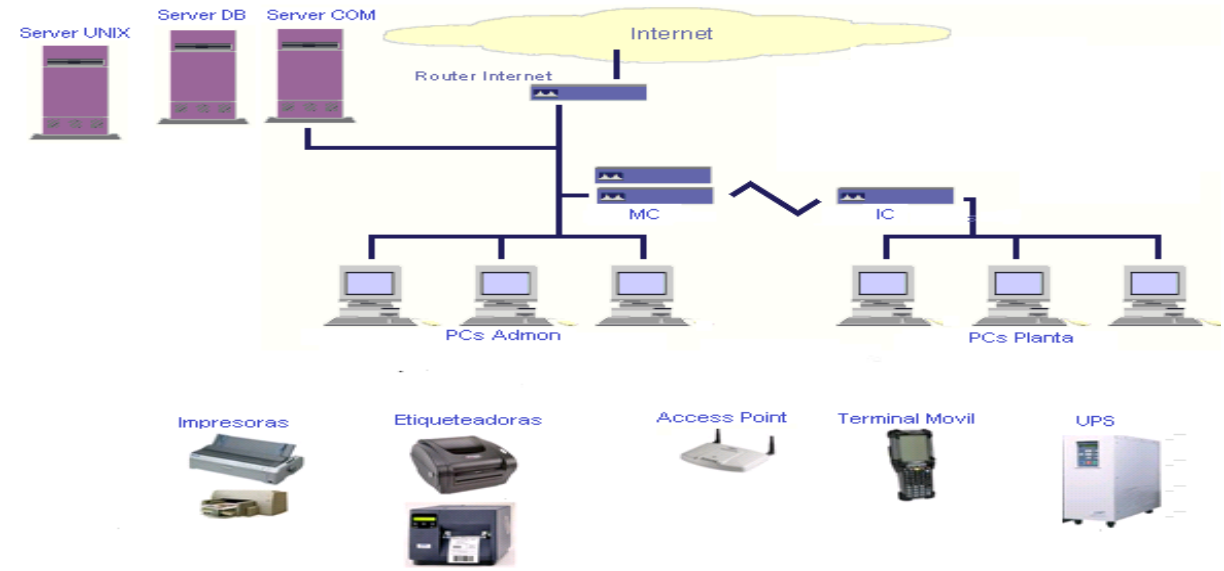
En el desarrollo de estas actividades RYMCO cumple las leyes, es un buen ciudadano buscando la satisfacción de sus empleados, accionistas y de la comunidad.

5.5.3 **Visión.** RYMCO S.A desea ser un gran proveedor de alta confiabilidad y preferencia para el sector salud por medio de procesos productivos y alianzas comerciales lo cual genere una alta rentabilidad que permita el desarrollo empresarial, con su permanencia y crecimiento.

La política del SGSI debe tener en cuenta el marco legal de RYMCO S.A comercialización de productos médicos para un solo uso.

5.5.4 **Estructura del Área De Sistema.**

Figura 1 Estructura del área de sistema de la empresa.



Fuente tomada del manual de calidad.

La red es un conjunto de equipos informáticos y software conectados entre sí para compartir los recursos y la información, asegurar la confiabilidad y la disponibilidad de la información.

La interconexión de ordenadores para poder acceder a los servicios y recursos, utilizamos Servidores con sistemas operativos Windows y Unix para soportar las base de datos SQL server y Unify 2.0, donde se almacena la información de los sistemas SBA15 y SINPRO16. El registro de datos se hace a través de Pc y Terminales móviles con tecnología Wifi segura.

Se dispone de un sistema regulado de corriente eléctrica, suministrado por una UPS de 15KVA central para todos los equipos de cómputo.

Server UNIX: Servidor compaq ML 350, disco duro 160 GB, 2 GB de RAM, Tape Backup 12 GB, Sistema operativo Unix 5.0 Tiene instalado el sistema de producción SIMPRO, el lenguaje de programación ACCELL/IDS y la base de datos Unify 2.0

Server DB: Servidor DELL powerEdge T710, procesador Intel dual core 3GB, 3 discos de 76GB en array 5, 8GB de RAM, fuente poder redundante, garantía hasta Dic 2014, con Windows server 2008 R2, encargado de manejar las bases de datos el SBA y otros software, con el software SQL server 2008

---

15 ***SBA***. Sistema Básico Visual Basic de Administración.

16 ***SINPRO***. Nombre asignado al software de UNIX.

Server COM: Servidor DELL powerEdge T710, procesador Intel dual core 3GB, 3 discos de 76GB en array 5, 8GB de RAM, fuente poder redundante, garantía hasta Dic 2014, encargado de controlar acceso de los usuarios a la red con Windows server 2008 R2, controlar el acceso a internet con Forefront 2010, mensajería unificada con Exchanger server 2010, consola de antivirus con McAfee. Para 80 usuarios.

Router Internet: conexión a internet, canal dedicado de 4GB con reusó 1:1, proporcionado por IFX

MC: Centro principal de cableado, para cubrir las áreas de administración, calidad y planta 1, proporciona conexión a la red de datos y teléfonos, tiene 1 SwtchsNetgear de 48 puertos y otro 24 puertos, Router de internet.

IC: Centro de cableado secundario, para cubrir las áreas de despachos, repuestos, planta 2 y 3, proporciona conexión a la red de datos y teléfonos, tiene un swicthNetgear de 24 puertos, conectado por fibra óptica y redundante en cobre al MC

Pc Admón.: son computadores de escritorio para ingresar al SBA, SINPRO, correo electrónico, office e internet. Las características de estos equipos son: procesador Intel dual CORE, 4 GB de RAM, 250 GB Disco Duro, con sistema operativo Windows 7 profesional y Office 2010, Antivirus McAfee.

Pc Planta: son computadores de escritorio para ingresar al SBA, SINPRO, correo electrónico y office. Las características de estos equipos son: procesador Intel Pentium 4, 1 GB de RAM, 40 GB Disco Duro, con sistema operativo Windows XP profesional y Office 2010, Antivirus McAfee.
Impresoras: utilizadas para la impresión de listados, ubicadas en cada área de la compañía, impresoras de tinta y matriz de punto.

Etiquetadoras: son impresoras de códigos de barras, ubicadas en las secciones de inyección, ensamble y empaque para la impresión de stiker para control de productos en proceso y terminados

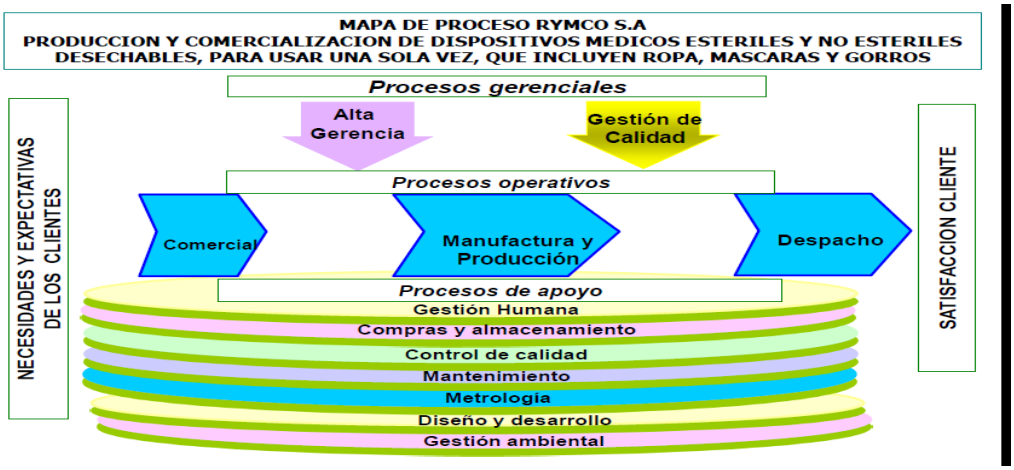
Access Point: son dispositivos para la red inalámbrica, utilizados para proporcionar conexión de la red LAN a las terminales Móviles, ubicados en las áreas de planta1, planta2, planta3, despachos y materias primas.

Terminales Móviles: son dispositivos para la red inalámbrica, utilizados para dar acceso al software SBA y al SINPRO

Ubicados en las áreas de planta1, planta2, planta3, esterilización y despachos.

5.5.5 **Descripción de los Procesos en Rymco.**

Figura 2 Descripción del proceso de RYMCO S.A



Fuente: manual de instrucción de calidad de la empresa

La gestión de aseguramiento: contempla los requisitos de calidad de sus productos para la satisfacción de los clientes de acuerdo a las expectativas de la alta dirección de la compañía para cumplir los requisitos del cliente y legales se define el plan estratégico, la política y los objetivos de la calidad los cuales deben ser coherentes entre si e incluir la mejora continua.

1. Procesos operativos: El objetivo de este proceso es el establecimiento comercial entre cliente y la empresa para el desarrollo de la ejecución y fabricación de los productos médicos mediante las necesidades y expectativas de los clientes para su satisfacción, incluyen los procesos comerciales, manufactura y producción y el despacho mediante el cumplimiento y ejecución de las órdenes de producción.

2. Procesos misionales: El objetivo de este proceso es asegurar la confiabilidad y trazabilidad de la fabricación de los productos, por lo tanto controlar los factores que lo determinan: Personal, Instalaciones, condiciones ambientales, inspecciones, Equipos, Trazabilidad de la mediciones, muestreo.

3. Proceso gestión apoyo (Talento humano): El objetivo de este proceso es asegurar el establecimiento de los parámetros necesarios para lograr un talento humano competente y comprometido con los objetivos de la organización. En donde se definen los cargos críticos, y perfiles de la empresa, para establecer los criterios del proceso de selección de personal, realizar evaluaciones de competencia, ejecutar capacitaciones o actividades de formación a su respectiva evaluación entre los cuales tenemos:Definir cargos críticos y perfiles.

a) Selección de personal

b) Evaluación de competencia de personal
c) Desarrollo de capacitaciones
d) Evaluaciones y eficacia

4. Gestión de la calidad: El objetivo de este proceso de gestión de calidad es establecer, documentar, implementar y mantener un sistema de gestión para la empresa que cumpla con las necesidades de sus clientes y mejora la gestión de la compañía, generando una sinergia entre los procesos. El sistema de gestión que aplica para esta empresa basada en las normas internacionales ISO 9001:200017.

5. Mantenimiento: El objetivo de este proceso es asegurar el mantenimiento preventivo de los equipos, software e instalaciones de la empresa, además de un plan de contingencia en caso de que se presente alguna falla en los mismos y que pueda llegar a retrasar o afectar de alguna manera la operatividad de las instalaciones.

Tener claro las terceras partes y su influencia sobre l seguridad de la información, es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben contemplar también dentro del alcance del sistema.

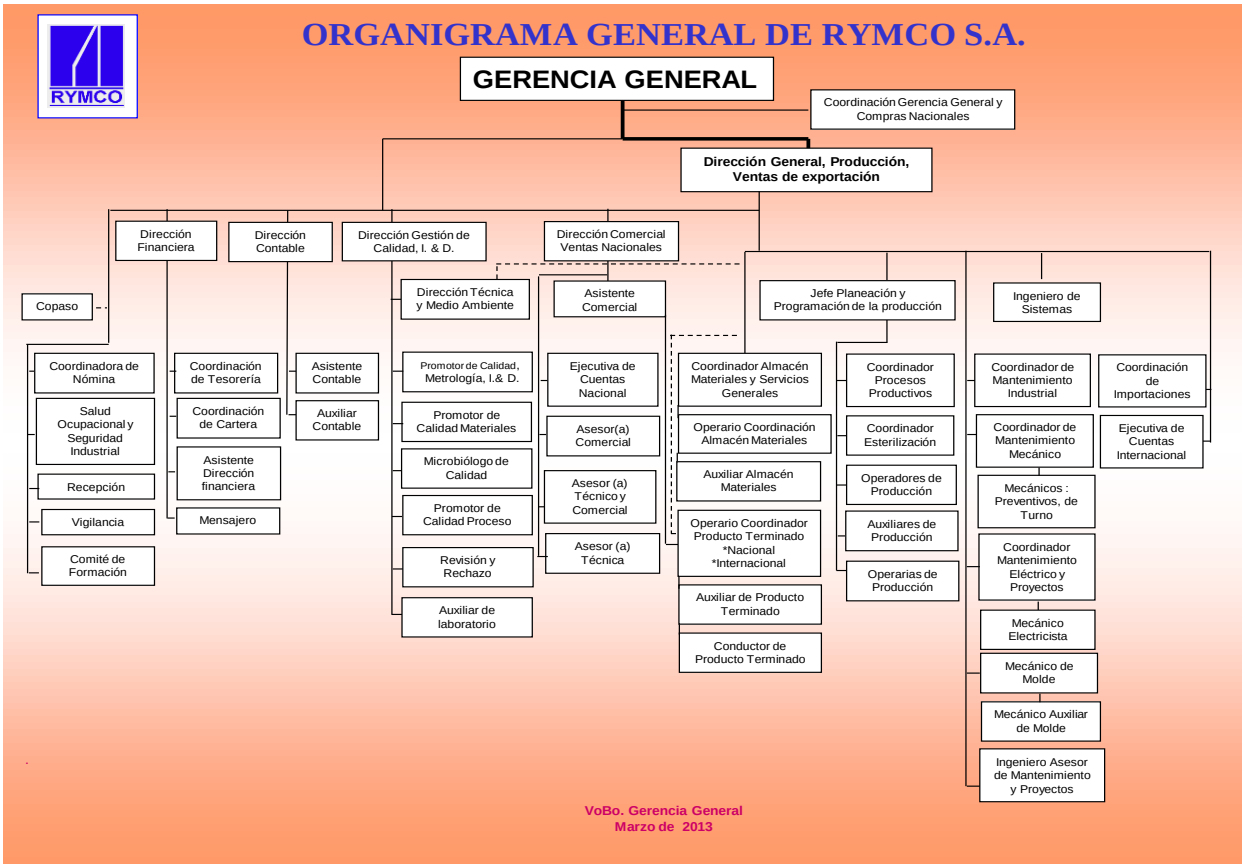
Crear mapas de redes y sistemas, definir la ubicación física y disponer de organigrama organizativo, facilitan establecer con claridad el alcance del SGSI.

Para el caso de RYMCO S.A sugerimos que el alcance del SGSI se enfoque en los procesos misionales, típicamente definidos como:

- ✓ Recepción de pedidos
- ✓ Generación de órdenes de producción
- ✓ Ejecución de órdenes
- ✓ Planeación de muestreo
- ✓ muestreo
- ✓ despacho

17 **Norma ISO 9001:2000. Norma de sistema de aseguramiento de la calidad.**

Figura 3 El organigrama de la empresa RYMCO S.A



Fuentes: manual de calidad ISO *9001:2005 empresa.*

5.5.6 **Necesidad de la Seguridad de la Información.** Diseñar, establecer, documentar, liderar, y mantener el SGSI en el área de sistema es importante para la empresa RYMCO S.A porque le representa una ventaja competitiva, flujo de caja, productividad, rentabilidad, y cumplimiento legal; al asegurar que la información, los procesos, la imagen corporativa y sistemas de apoyo son activos importantes que deben resguardarse.

6 METODOLOGÍA

Se realizara una investigación de tipo viable que consiste en un análisis y de una propuesta de diseño de un SGSI en el área de sistemas de la empresa RYMCO S.A basado en la norma ISO IEC/27001:2013, utilizando metodologías de buenas prácticas y promover la mejora continua y compromiso de la alta gerencia en el liderazgo para que se cumplan los objetivos diseñados de este proyecto.

En la primera etapa del proyecto se desarrollara un análisis de riesgos actuales y potenciales que está expuesto los activos de la empresa RYMCO S.A en cuanto a las vulnerabilidades y amenazas. En este estudio clasificaremos los activos que posea la empresa.

En la segunda etapa y de acuerdo a los resultados obtenidos de la evaluación de riesgos, se diseñara un SGSI en el área de sistema de acuerdo a las necesidades de la empresa. El empleo de la matriz de riesgo evidenciara las probabilidades altas, medias y bajas, dependiendo de la frecuencia de ocurrencia del mismo. De la misma manera se determinara se clasificara el impacto como leve, moderado o catastróficos según el caso, para identificar las acciones y procedimientos en la realización del diseño del SGSI.

6.1 CICLO PHVA

Definición: el ciclo PHVA (o PDCA en inglés), es una herramienta de mejora continua, diseñada por el Dr. Walter Shewhart en 1920 y presentada por Deming a partir de 1950, la cual se basa en un ciclo de 4 pasos: Planificar, Hacer, Verificar y Actuar.

Planear: establecer los objetivos y los procesos necesarios para conseguir los resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

Hacer: Fomentar la necesidad de implementarlo en los procesos.

Verificar: analizar el seguimiento y medición de los procesos, respetar las políticas, los objetivos y los requisitos.

Actuar: tomar acciones para la mejora continua.

6.2 CICLO PHVA PARA EL SGSI

El diseño metodológico de este trabajo se basa en la metodología PHVA de la norma ISO 27001 para los SGSI, en la figura se pone en contexto la metodología propuesta en este documento dentro de cada etapa del ciclo.

Planear*:* dentro de los estudios de situaciones tendremos.

- ✓ Definir el alcance y los objetivos del SGSI.
- ✓ Definir la política de seguridad.
- ✓ Metodología para la evaluación de riesgos.
- ✓ Inventario de los activos.
- ✓ Identificar las amenazas y vulnerabilidades.
- ✓ Identificar el impacto.
- ✓ Análisis y evaluación de riesgos.
- ✓ Selección de los controles.

Figura 4 Ciclo PHVA

Fuentes:http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

Hacer**:** entre los cuales tendremos

- ✓ Definir el plan de tratamiento de riesgo.
- ✓ Diseñar el plan de tratamiento de riesgo.

- ✓ Diseñar los controles.
- ✓ Formar y concientizar.
- ✓ Poner en operación el SGSI.

Verificar: implantaremos los siguientes.

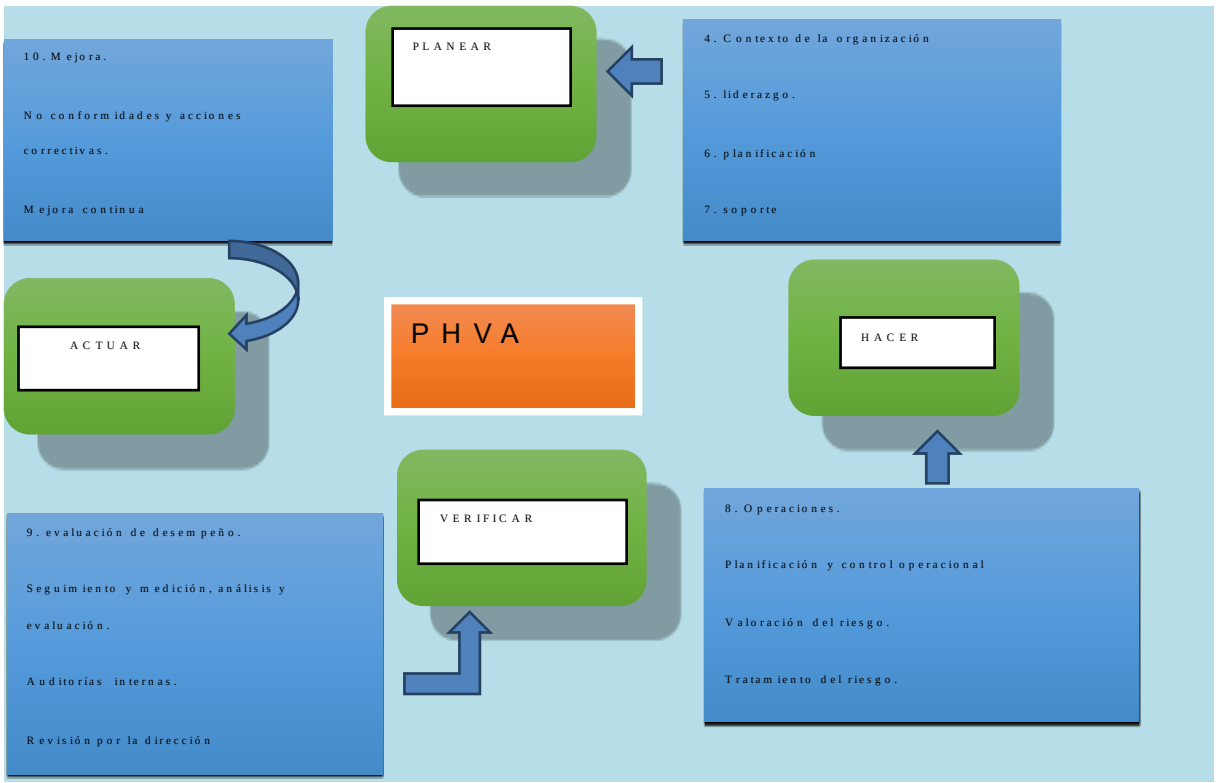
- ✓ Revisar el SGSI.
- ✓ Medir la eficacia de los controles.
- ✓ Revisar los riesgos residuales.
- ✓ Realizar auditorías internas del SGSI.
- ✓ Registrar las acciones y evento
- ✓

Actuar: para los cuales tendremos los siguientes.

- ✓ Diseñar mejoras.
- ✓ Acciones correctivas.
- ✓ Acciones preventivas.
- ✓ Comprobar la eficacia de las acciones.

Dentro de la parte metodológica es importante la correlación metodológica de la norma ISO 27000 en el siguiente cuadro

Figura 5 Correlación metodológica ISO 27001:2013.



Fuente el Autor

7 DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

7.1 INICIO DEL PROYECTO

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información y que se cumpla:

a) Asegurar que se establezcan las políticas de la seguridad
b) Los objetivos de la seguridad de la información
c) Que los requisitos se integren al sistema de gestión de la seguridad de la información
d) Que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles
e) Asegurar que se logre los objetivos esperados.
f) Contribuir a la eficacia del sistema de gestión de la seguridad de la información
g) Por ultimo promover la mejora continua demostrando liderazgo.
h) Diseñar el plan de contingencia, para mitigar los riesgos en el área de sistemas.

7.1.1 **Etapa de Planeación del Proyecto.** En la etapa de planeación se define el alcance del sistema dentro de la organización y las políticas y lineamientos sobre los que se desarrollara, se presentan herramientas para la identificación, análisis y evaluación de riesgos, según el impacto de cada uno y el tipo de información que se afectaría, de igual forma es objetivo de esta etapa definir la forma de tratamiento de los riesgos identificados.

8 ALCANCE DEL DISEÑO DEL SGSI

El alcance se ha delimitado en este proyecto para el AREA DE SISTEMAS, cuyo objetivo es lograr la implementación a mediano plazo.

8.1 *CLASIFICACION DE ACTIVOS DE INFORMACION DEL AREA DE SISTEMAS*

Es importante identificar todos los recursos de la red que podían verse afectados por un problemas de seguridad. Podemos mencionar los siguientes ejemplos de activos asociados a sistemas de información:
Confidencialidad.

8.2 RECURSOS DE INFORMACIÓN

bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.

8.3 RECURSOS DE SOFTWARE

Software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.

- ✓ Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles y módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

- ✓ Servicios: Servicios informáticos y de comunicaciones, utilitarios generales, por ejemplo: calefacción, iluminación, energía eléctrica, aire acondicionado.

- ✓ Recursos humanos: El personal que labora dentro de la empresa representado en 125 empleados

9 INVENTARIO DE LOS ACTIVOS DE LA INFORMACIÓN.

Representados en los datos obtenidos de la empresa RYMCO S.A, de los proceso identificados como sus activos, tipos y los responsables de los mismos.

Tabla 1 Inventario de los activos.

RYMCO	**INVENTARIO DE ACTIVOS DE LA INFORMACION**					Código: SGSI001	
	CONFIDENCIALIDAD= C	SGSI				Fecha 05.15.2014	
	INTEGRIDAD= I					página 1-1	
	DISPONIBILIDAD = D						
Proceso	Identificación de los activos	tipo de activo	propietario/ responsable	Ubicación	C	I	D
	Personal técnico	Usuario	Director de planeación	Oficina de planeación	SI		
	Instalaciones físicas	Organizacional	Jefe de producción	Planta			SI
	Sistemas operativos y plataforma	Software	Jefe de sistema	Servidor			SI
	Computadores	Hardware	Jefe de sistema	Sistema			SI
	Imagen organizacional	Organizacional	Director técnico	Programación	SI		
	Información del cliente	Información	Director técnico	BD del cliente		SI	
	Información de la orden de producción	Información	Director técnico	Programación			SI
	datos	Información	Director técnico	Servidor	SI		
	Norma de referencia permisible	Información	Director técnico	Servidor		SI	
	Conclusión de la orden	Información	Director técnico	Servidor			SI

Fuentes: el autor

9.1 *REQUISITOS DE CONFIABILIDAD*

Tabla 2 Requisitos de confiabilidad

REQUISITOS DE CONFIABILIDAD ©		
VALOR DEL ACTIVO	CLASE	DESCRIPCION
BAJO	Disponible al publico	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procedimientos de la información y los recursos del sistema están disponibles dentro de la organización con estrictas variables con base a las necesidades de la empresa
MEDIO	Para uso interno exclusivamente o uso restringido solamente	El daño o modificación no autorizada no es crítico pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.
ALTO	Confidencial o estrictamente confidencial	La información no sensible y las instalaciones de procedimientos de la información y los recursos del sistema están disponibles solo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procedimiento de información y los recursos del sistema están disponibles solo sobre la base de la necesidad estricta del conocimiento.

Fuentes 1 http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

9.2 REQUISITOS DE INTEGRIDAD

Tabla 3 Requisitos de integridad.

REQUISITOS DE INTEGRIDAD (I)		
VALOR DEL ACTIVO	CLASE	DESCRIPCION
BAJO	Baja integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el impacto en la empresa es insignificante o menor
MEDIO	Integridad mediana	El daño o modificación no autorizada no es crítico pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.
ALTO	Integridad alta o muy alta	El daño o modificación no autorizada es crítica para la aplicaciones empresariales y el impacto en la empresa es importante y podría conllevar a la falta grave o total de la aplicación empresarial

Fuentes 2 http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos.Anexos

9.3 REQUISITOS DE DISPONIBILIDAD

Tabla 4 Requisitos de disponibilidad.

REQUISITOS DE DISPONIBILIDAD (A)		
VALOR DEL ACTIVO	CLASE	DESCRIPCION
BAJO	Baja disponibilidad	Se puede tolerar que el activo no esté disponible por más de un día.
MEDIO	Disponibilidad mediana	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día
ALTO	Alta disponibilidad	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas o incluso menos

Fuentes http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

9.4 INTERPRETACION DEL INVENTARIO DE LOS ACTIVOS

Tabla 5 Inventario de los activos.

RYMCO	INVENTARIO DE ACTIVOS DE LA INFORMACION					Código: SGSI001	
	CONFIDENCIALIDAD = C	SGSI				Fecha 05.15.2014	
	INTEGRIDAD = I					página 1-1	
	DISPONIBILIDAD = D						
Proceso	Identificación de los activos	tipo de activo	propietario/ responsable	Ubicación	C	I	D
	Pers+B6:H15onal técnico	Usuario	Director de planeación	Oficina de planeación	alto	alto	medio
	Instalaciones físicas	Organizacional	Jefe de producción	Planta	medio	alto	alto
	Sistemas operativos y plataforma	Software	Jefe de sistema	Servidor	medio	alto	medio
	Computadores	Hardware	Jefe de sistema	Planta	alto	medio	alto
	Imagen organizacional	Organizacional	Director técnico	Programación	alto	alto	alto
	Información del cliente	Información	Director técnico	BD del cliente	alto	medio	medio
	Información de la orden de producción	Información	Director técnico	Programación	alto	medio	medio
	datos	Información	Director técnico	Servidor	alto	alto	alto
	Norma de referencia permisible	Información	Director técnico	Servidor	bajo	medio	medio
	Conclusión de la orden	Información	Director técnico	Servidor	alto	medio	bajo

Fuentes el Autor

10 IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo contempla inicialmente la determinación de los activos de información dentro del alcance del SGSI, teniendo en cuenta la ubicación, responsable y funciones. De igual manera se deben determinar las amenazas, vulnerabilidades e impacto en la organización, por la posible pérdida de confiabilidad, integridad, y disponibilidad sobre los activos.

De acuerdo a lo anterior se realiza un inventario de activos relacionando cada proceso de la organización contemplando en el alcance del SGSI (Anexo 3), los activos hacen referencia a: personal de la organización, imagen organizacional, información, sistema de información, procesos, productos, aplicaciones y entorno físico.

Además de ejemplo y para poner en contexto la aplicación de la metodología propuesta en el sector de RYMCO S.A, seleccionamos uno de los procesos gestión de apoyo (mantenimiento de software y hardware) para hacer el desarrollo de cada uno de los puntos.

Se estableció el inventario de activos para el proceso de ejecución de órdenes de acuerdo al formato diseñado en el anexo 3 el numeral 2.6.0 se realiza la identificación del impacto para complementar el formato.

Es importante tener claridad en los conceptos de amenazas y vulnerabilidad para identificar en el análisis de cada activo.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización Ejemplo: acceso no autorizados, código malicioso, spam, hackers, hurto por empleados, o no empleados, mal uso del sistema de procedimiento de la información, fraude, falla del sistema, negación del servicio, errores de usuarios, desastres, etc.

Vulnerabilidades: la debilidad de un activo o grupo de activos que pueden ser explotadas por una o más amenazas. Ejemplo: Falta de concientización, Falta de responsabilidades claras, Clasificación errónea de la información, Incapacidad de proporcionar, evidencias, Falta de control de cambio o de versión, Falta de mantenimiento, Identificación no adecuada, Falta de seguridad de los medios, Falta de protección física.

En el análisis de las amenazas y vulnerabilidades se requiere:

- realizar una lista de amenazas que puedan presentarse en forma accidental, o intencional, en la empresa con relación a los activos de

información. Diferenciar estas amenazas de las vulnerabilidades de los activos ya que el análisis debe radicar en las amenazas.

- Identificar los riesgos de los procesos. Es necesario analizar los riegos que se pueden presentar cuando se subcontrata un servicio o existe personal externo a la organización.

- Realizar un análisis del entorno en los fenómenos naturales, el ambiente geopolítico, el ambiente tecnológico, el ambiente ecológico y los aspectos socioculturales que rodea la organización para definir las amenazas a las que puede estar expuesto los activos.

Figura 6 Ilustración amenazas y riesgos identificados en RYMCO S.A.

Fuentes el Autor

10.1 ANÁLISIS Y EVALUACIÓN DEL RIESGO

Revisando en términos generales la información que se puede manejar en una empresa como RYMCO S.A como organización las amenazas se pueden clasificar en tres grupos:

- Externas: Intrusión a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación, de identidad, fraude, espionaje, sabotaje, robo de información entre otras.

- Internas: Generadas al interior de la organización, principalmente por el conocimiento de los colaboradores. Ejemplo: Alteración de la información, divulgación de la información, fraudes, robos, sabotaje, uso no autorizado del sistema de información, uso de la imagen corporativa sin autorización etc.

- Naturales: son generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, etc.

Como lo resalta la norma ISO 27002:2013 La seguridad de la información se logra establecer un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesita establecer, diseñar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debe realizar en conjunción con otros procesos de gestión de negocio.

La estimación del riego es el paso a seguir con el fin de valorar y determinar su importancia; puede ser cuantitativa al definir escalas de ocurrencia o cualitativa al usar escalas numéricas. El objetivo de esta etapa es obtener una lista de riegos identificados de acuerdo a la probabilidad de ocurrencia de una amenaza y de sus consecuencias de los impactos, ligadas a la vulnerabilidad existente a los activos de la información.

RIESGO = activo de información + probabilidad + impacto.

Lo ideal en este pasó utilizar la matriz de Análisis Modal de Fallos y Efectos AMFE18

18 *Análisis modal de fallos y efectos (AMFE) es un procedimiento de análisis de fallos potenciales en un sistema de clasificación determinado por la gravedad o por el efecto de los fallos en el sistema.*

Como paso previo a la descripción del método y su aplicación es necesario sentar los términos y los conceptos fundamentales como lo son la Detectabilidad, Frecuencia y Gravedad.

Detectabilidad: Este concepto es esencial en el AMFE. Si durante el proceso se produce una falla o cual "output" defectuoso se trata de averiguar la probabilidad que no lo detectemos pasando a etapas posteriores en el proceso, generando los consiguientes problemas y llegando en ultimo termino afectar al usuario final, en este caso el propietario del activo de información y si es caso a toda la organización

Frecuencia: mide la repetitividad potencial u ocurrencia de un determinado fallo, es lo que en términos de factibilidad o de prevención llamados la probabilidad de aparición del fallo.

Gravedad: mide el daño normalmente esperado que provoca el fallo en cuestión, según la percepción del propietario del activo y del equipo del SGSI, para que no sea objetivo del análisis

Tabla 6 Análisis y evaluación de riesgo AMFE

DETECTABILIDAD AMFE		
DETECTABILIDAD	CRITERIO	VALOR
Muy alta	Detección obvia	1
Alta	Facilmente detectable	2
Mediana	Detectable despues de varios controles	3
Mínima	Difícil detección	4
improbable	No puede detectar	5
FRECUENCIA AMFE		
FRECUENCIA	CRITERIO	VALOR
Muy baja improbable	Es concebible. No se ha presentado	1
Baja	Es poco probable, aunque se puede dar en el sistema	2
Moderada	Ocasionalmente	3
Alta	Se ha presentado con cierta frecuencia	4
Muy alta	Frecuentemente	5
GRAVEDAD AMFE		
GRAVEDAD	CRITERIO	VALOR
Muy baja imperceptible	Fallo de pequeña importancia, efecto imperceptible	1
baja	Repercusiones irrelevantes apenas perceptible	2
Moderada	Repercusiones de relativa importancia	3
Alta	Repercusiones elevadas criticas	4
Muy alta	Muy crítico serio.	5

Fuentes HTTP//www.pdcahome.com/guia de uso AMFE/FORMATO

10.2 INDICE DE PRIORIDAD DE RIESGO (IPR)

El índice de prioridad del AMFE incorpora el factor detectabilidad. Por tanto, tal índice es el producto de la frecuencia por la gravedad y por la detectabilidad, siendo tales factores traducibles a un código numérico adimensional que permite priorizar la urgencia de la intervención, así como el orden de las acciones de control o tratamiento en este caso de seguridad de la información. Por tanto debe ser calculado por todas las causas de fallos.

IPR= D.G.F (los valores deben estar comprendido entre 1 a 50), en donde menor de 50 no requiere intervención, sino la incorporación de mejoras al proceso

Tabla 7 Matriz AMFE para el SGSI.

AMFE							
Elemento /causa	**Modo de fallo**	**Efecto**	**F**	**G**	**D**	**NPR = S*O*D**	**Acciones propuestas**
describir elemento	describir modo de fallo	describir efecto	1 a 10	1 a 10	1 a 10	**1 a 1000**	proponer acción de mejora si sale un NPR alto
falla del servidor	Código inadecuado	Error de trazabilidad	2	3	2	**12**	Ninguna
Falla de energía	Mal funcionamiento del servidor	Pérdida de tiempo	3	5	1	**15**	Ninguna
Alteración de los reportes	Mal reporte	Mal reporte	2	5	4	**40**	Disminuir G (implementar capacitaciones)
Divulgación de la información	Perdida de confiabilidad	Ruptura con el cliente	3	5	3	**45**	Disminuir G (encriptar los datos)
robo de información	Perdida de información	retraso	2	5	2	**20**	Disminuir G (Revisar los controles)
Falta de capacitación	incoherencia	Error de reporte	2	4	2	**16**	Disminuir G (Revisar la capacitación)
Falla del servidor reportes	equivocación	desconfianza	2	5	3	**30**	Disminuir G (Validación del software)
falta de tiempo	Mala identificación	quejas	4	2	2	**16**	Disminuir F (Mejorar los controles)
Falla no verificación de mail	Mal reporte	Problema de trazabilidad	2	5	3	**30**	Disminuir G (Mejorar los controles)
Acceso no autorizado	plagio	Rompimiento de confiabilidad	1	5	2	**10**	Ninguna
Alteración de reportes	Reporte no confiable	Mal reporte	2	5	3	**30**	Disminuir G (Mejorar los controles)
sabotaje	Perdida de información	Quejas del cliente	1	5	3	**15**	Ninguna
Código malicioso	Perdida por fallos	Aumento de costo	2	5	3	**30**	Disminuir G (Mejorar los controles)
Virus malicioso	Perdida de datos por el pc	Problemas de trazabilidad	3	4	2	**24**	Disminuir G (Mejorar los controles)
Uso indebido de imagen	Perdida de estatuto	Mala imagen	1	5	4	**20**	Disminuir G (Revisar estatutos legales)
Falta de energia inundación	Incumplimiento de entrega	Aumento de costo	5	4	1	**20**	Disminuir F (Mejorar los controles)

Fuentes HTTP//www.pdcahome.com/guia de uso AMFE/FORMATO

10.3 RESULTADOS

En el SGSI los riesgos con un IPR[19] mayor de 15 presentan una gravedad alta que perjudica a la organización y la calidad de su proceso. En cuanto a los resultados arrojados los malos reportes, la pérdida de confiabilidad, las equivocaciones, los incumplimientos en las entregas y los malos reportes requieren tratamiento especial, debido a su gravedad.

Los IPR inferiores a 50 necesariamente no requieren intervención inmediata según los límites de SGSI, salvo la necesidad sean para introducir mejoras en el sistema de gestión.

Tabla 8 Nivel AMFE resultados.

Elemento /causa				
describir elemento	F	G	D	NIVEL
falla del servidor	2	3	2	BAJO
Falla de energía	3	5	1	MEDIO
Alteración de los reportes	2	5	4	ALTO
Divulgación de la información	3	5	3	ALTO
robo de información	2	5	2	ALTO
Falta de capacitación	2	4	2	MEDIO
Falla del servidor reportes	2	5	3	ALTO
falta de tiempo	4	2	2	MEDIO
Falla no verificación de mail	2	5	3	ALTO
Acceso no autorizado	1	5	2	BAJO
Alteracion de reportes	2	5	3	ALTO
sabotaje	1	5	3	MEDIO
Código malicioso	2	5	3	ALTO
Virus malicioso	3	4	2	ALTO
Uso indebido de imagen	1	5	4	ALTO
Falta de energia inundación	5	4	1	ALTO

Fuentes el Autor

19 ***IPR.*** *Es igual a P.G.D, Probabilidad de ocurrencia, Gravedad de fallos, Probabilidad de no detención. Permite evaluar los diferentes niveles de riesgo y ordenar según sus prioridades.*

11 IDENTIFICACIÓN DEL IMPACTO

Una vez identificado los activos de información que posee RYMCO S.A para cada uno de los procesos que se ha decidido incluir dentro del alcance del SGSI, se debe identificar cual sería el impacto que tendría en su respectivo proceso la pérdida o alteración de cada uno de los activos identificados.

Entiéndase impacto como el grado en el que se ve afectado determinado sistema, en este caso proceso, al alterar uno de sus componentes, para este caso activos de información. A mayor correlación entre el resultado del proceso y la alteración del activo, el impacto de ese activo será mayor se concluye lo siguiente:

1. Los malos reporte generan pérdidas considerables para la empresa cuyo impacto y consecuencias generan inventarios no reales.

2. Los incumplimientos en las entregas generan un impacto negativo por parte de los clientes que piensan en cambiar de proveedor.

3. La mala imagen organizacional produce un impacto negativo para la empresa puesto que peligra su permanencia como empresa en el mercado.

12 PLAN DE CONTINGENCIA

12.1 *ALCANCE*

Para todas las personas que trabajan y se encuentran dentro de las instalaciones de la empresa RYMCO S.A.

12.2 *OBJETIVO*

El propósito de este plan de contingencia del diseño del SGSI en el área de sistemas de la empresa RYMCO S.A, se delinearan una serie de controles, para mitigar los riesgos en el área de sistema que le puedan generar perjuicios a la empresa y pongan en riesgo su permanencia operacional.

12.3 *CONTROLES PARA EL PLAN DE CONTIGENCIA*

Para la consecución de los objetivos del plan de plan de contingencia se establecen los siguientes controles:

Evaluación: si bien es cierto que dentro del análisis de riesgo evaluado inicialmente los valores resultantes del IPR no superaron 50 por lo que no requiere intervención inmediata, pero se contemplaran unas acciones de mejoras para mitigar los riesgos como corte de energía, fallas en la red de voz y datos, fallas en el hardware y el software, sabotaje entre otros.

Planificación: para el diseño del SGSI, el esquema general del plan de contingencia de los sistemas de información, se planificaran las siguientes tres fases:

a) Fase 1 mitigar el riesgo
b) Fase 2 recuperación de contingencia, cuanto se generen fallos
c) Fase 3 organización de los sistemas de alerta contra fallo

- ✓ Pruebas de viabilidad: los métodos para las pruebas del plan de contingencia se implementarán las siguientes:

a) Prueba específica
b) Prueba de escritorio
c) Simulación en tiempo real.

Para la eficacia del plan de contingencia este debe estar aprobado por la alta gerencia de RYMCO S.A, y de la misma manera se verificara si están establecidas las responsabilidades del plan contingencia. Finalmente se debe realizar las pruebas finales el cual debe ser una prueba integrada que involucre secciones múltiples del área de sistemas e instituciones externas. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentran los resultados de las pruebas, con las metas planteadas, para así realizar las correcciones.

- ✓ Ejecución: desarrollo del plan de contingencia informático de los sistemas de información contemplados en este proyecto de diseño de un SGSI en el área de sistema de la empresa RYMCO S.A
  .
- ✓ Recuperación: se tendrán presente 9 etapas que facilitan la recuperación de los datos de la empresa

1. Análisis y selección de las operaciones críticas
2. Análisis y selección de las operaciones críticas

3. Identificación de los procesos de cada operación
4. Lista de documentos utilizados en la operación
5. Especificación de los escenarios donde ocurren los problemas
6. Determinar y detallar las medidas preventivas
7. Formación y funciones de los grupos
8. Desarrollo de los planes de acción
9. Preparación de las listas de personas e instituciones para comunicarse.
10. Pruebas y monitoreo.

12.4 MEJORAMIENTO CONTINÚO

1. Establecer el SGSI se ha establecido un plan de contingencia de acuerdo a las amenazas declaras en la empresa RYMCO S.A bajo la norma ISO IEC/27001:2013

2. Mantener la mejora continua. Plan para la continuidad de negocio se debe proveer las personas necesarias para mantener y mejorar el plan de contingencia

3.
4. Monitorear y revisar el SGSI. Es necesario que se revise el plan de contingencia por parte de dirección de la empresa

5. Implementar el SGSI y operarlo describiéndolo paso a paso la implementación de las estrategias para las soluciones de las amenazas presentadas

6. Finalmente se debe recomienda implementar el plan de respaldo, que debe contemplar serias medidas preventivas antes que se establezca una amenaza y cuyo propósito es evitar la materialización, el plan de emergencia que corresponden a las acciones que se deben realizar cuando se presente el siniestro.

12.5 HACER PHVA

Bajo el esquema metodológico PHVA, Crearemos un plan medidas necesarias documentadas utilizadas por las normas IEC/27001 que faciliten la consecución de los objetivos esperados para tal fin.

13 PLAN DE TRATAMIENTO DEL RIESGO

La gestión de los riesgos es un proceso en el cual diseñamos las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos analizados e identificados, de forma que las consecuencias que puedan generar sean eliminadas o, si esto no es posible, se puedan reducir al máximo posible. El resultado obtenido del análisis de riesgo nos lleva a determinar el criterio, de los riesgos aceptables y por consiguiente a determinar lo que son totalmente inaceptables.

Estos son los tratamientos que requieren acciones diferentes:

- Mitigar el riego: los reduciremos mediante la implementación de controles.
- Asumir el riesgo: en nuestro quien lo asume es la dirección de RYMCO S.A pero desde luego con valores aceptables y controlados.
- Establecer un plan de contingencia para mitigar ese riesgo

14 PASOS PARA MITIGAR LOS RIESGOS EN RYMCO S.A

- Establecer los controles apropiados, mediante el catálogo de las Buenas Practicas de la ISO/IEC 27002. (133 Controles posibles), de igual forma podemos añadir otros que RYMCO S.A considere necesario.
- Diseñaremos los procedimientos para implementar los controles y su mantenimiento.
- Verificación que los controles estén correctamente redactados
- Es necesario establecer indicadores para medir la eficacia de esos controles en RYMCO S.A.

14.1 SELECCIÓN DE CONTROLES

Para la selección de esos controles para nuestro proyecto que estamos diseñando nos sirven esos controles que podamos impedir que los usuarios de los sistemas comentan errores o que dañen intencionalmente los activos de RYMCO S.A

Tabla 9 Checklist aplicado al proyecto de la ISO IEC/27001:2013

Requisito	contexto	Cumple	No cumple	recomendaciones
5.	POLITICAS DE SEGURIDAD.			
5.1	Directrices de la Dirección en seguridad de la información.		No cumple	Requiere establecer las directrices, para el cumplimiento de las políticas de seguridad
5.1.1	Conjunto de políticas para la seguridad de la información		No cumple	Diseñar las políticas necesarias, para establecer las y se cumplan.
5.1.2	Revisión de las políticas para la seguridad de la información.		No cumple	Diseñadas estas revisar si son las necesarias para el cumplimiento de los objetivos.
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION			
6.1	Organización interna.		No cumple	Documentar, velar por su actualización,

				para garantizar la seguridad de la información.
6.1.1	Asignación de responsabilidades para la seguridad de la información.	Cumple		Designar el líder para el caso el Ing. Del área de sistema para el establecimiento y control de los requisitos necesarios.
6.1.2	Segregación de tareas.		No cumple	Se requiere segregar las tareas con el fin de reducir modificación de personas no autorizadas.
6.1.3	. Contacto con las autoridades		No cumple	Se debe mantener contacto con la autoridad pertinente
6.1.4	Contacto con grupos de interés especial.		No cumple	Requiere tener contacto con personas de la especialización.
6.1.5	Seguridad de la información en la gestión de proyectos.	Cumple		La seguridad se lleva a cabo bajo la gestión del proyecto para poder alcanzar los objetivos esperados.
6.2	. Dispositivos para movilidad y teletrabajo.		No cumple	Requiere establecer una política para los dispositivos móviles.
6.2.1	Política de uso de dispositivos para movilidad.		No cumple	Requiere adoptar las políticas, dado que no las tiene y es fundamental.
6.2.2	Teletrabajo.		No cumple	La preservación de la información en el sitio de trabajo es fundamental.
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
7.1	Antes de la contratación.	Cumple		El compromiso de recursos humano con la gestión es fundamental para la consecución de los objetivos.
7.1.1	Investigación de antecedentes.		No cumple	Requiere realizar la verificación de los antecedente de las personas que va a contratar la empresa
7.1.2	Términos y condiciones de		No cumple	Requiere que los acuerdos al momento de

	contratación.			contratar estén contemplados con la seguridad de la información.
7.2	Durante la contratación.		No cumple	Concientizar a todo el personal contrato de la seguridad de la información, para que conozca los lineamientos de la organización.
7.2.1	Responsabilidades de gestión.		No cumple	Es importante que la dirección vele por el cumplimiento de la aplicación de la seguridad de la información.
7.2.2	Concienciación, educación y capacitación en asegurar de la información.		No cumple	Todo el personal de la organización de recibir capacitación de la seguridad de la información.
7.2.3	Proceso disciplinario.		No cumple	Es necesario que se establezcan procesos disciplinarios por violación de la seguridad de la información.
7.3	Cese o cambio de puesto de trabajo.		No cumple	Es necesario que la empresa proteja su información cuando finaliza el contrato laboral con el empleado
7.3.1	Cese o cambio de puesto de trabajo.		No cumple	El cambio de puesto de trabajo debe estar contemplado, ya que al cambiar de puesto las responsabilidades pueden ser distintas.
8.	GESTIÓN DE ACTIVOS.			
8.1	Responsabilidad sobre los activos.		No cumple	Se debe establecer las responsabilidades de los activos, para un mejor control.
8.1.1	Inventario de activos.	Cumple		Se debe inventariar los activos de la empresa y se deben actualizar.
8.1.2	Propiedad de los activos.	Cumple		Es importante asignar la propiedad del activo y debe hacer en el inventario.
8.1.3	Uso aceptable de los activos	Cumple		El uso aceptable del activo debe estar documentado e identificado.
8.1.4	Devolución de activos.		No cumple	Todos los activos de la organización deben ser devueltos por el empleado al

				momento de su retiro.
8.2	Clasificación de la información. Contexto	Cumple		La clasificación del activo debe estar de acuerdo a su importancia y criticidad del mismo.
8.2.1	Directrices de clasificación.		No cumple	Es importante establecer unas directrices al momento de clasificar los activos.
8.2.2	Etiquetado y manipulado de la información.	Cumple		Es vital que los activos estén etiquetados para un mejor control de los inventarios.
8.2.3	Manipulación de activos.		No cumple	Se recomienda que el manejo de los activos deba estar documentado, clasificado e implementado.
8.3	Manejo de los soportes de almacenamiento.		No cumple	Se recomienda que por seguridad deban existir políticas en cuando al manejo de soportes de almacenamientos.
8.3.1	Gestión de soportes extraíbles.		No cumple	Se debe implementar controles para dispositivos tipos USB, uso de ellos mediante controles establecidos.
8.3.2	Eliminación de soportes		No cumple	Los soportes deben estar siempre disponibles y esta es una valencia que presenta la empresa.
8.3.3	Soportes físicos en tránsito		No cumple	Se recomienda garantizar de manera segura el transporte de los activos, dedo la criticidad del mismo.
9.	CONTROL DE ACCESOS.			
9.1	Requisitos de negocio para el control de accesos.		No cumple	Se recomienda limitar el acceso a la información, es importante que ella este protegida.
9.1.1	Política de control de accesos.		No cumple	Se recomienda establecer, documentar y revisar las políticas del control de acceso.
9.1.2	Control de acceso a las redes y servicios asociados.	Cumple		Solo se debe permitir el acceso a las personas autorizadas a la red, dado los riesgos que se pueden generar.

9.2	Gestión de acceso de usuario.		No cumple	Se recomienda restringir el acceso a la red, solo con privilegios otorgados.
9.2.1	Gestión de altas/bajas en el registro de usuarios.		No cumple	Se recomienda velar por la gestión de altas y bajas de acceso a la red inmediatamente.
9.2.2	Gestión de los derechos de acceso asignados a usuarios.		No cumple	Se debe documentar los accesos otorgado a los usuarios, como control del área de sistema.
9.2.3	Gestión de los derechos de acceso con privilegios especiales.		No cumple	Los accesos de privilegios especiales deben ser otorgados de manera controlada.
9.2.4	. Gestión de información confidencial de autenticación de usuarios.	Cumple		Este se recomienda usarlo mediante un proceso de gestión formal.
9.2.5	Revisión de los derechos de acceso de los usuarios.		No cumple	Se recomienda que el propietario de revise periódicamente el acceso de los usuarios.
9.2.6	Retirada o adaptación de los derechos de acceso		No cumple	Se deben retirar todos los acceso de los usuarios al terminar su contacto...
9.3	Responsabilidades del usuario.		No cumple	Se debe verificar que los usuarios respondan por las salvaguardas de su información.
9.3.1	Uso de información confidencial para la autenticación.	Cumple		Se recomienda garantizar que la información sea secreta, es fundamental dado la criticidad de ella.
9.4	Control de acceso a sistemas y aplicaciones.		No cumple	Se debe controlar que el acceso al sistema, solo para las personas autorizadas.
9.4.1	Restricción del acceso a la información.		No cumple	Se recomienda que el acceso al sistema cumpla con la restricción a personas no autorizadas.

9.4.2	Procedimientos seguros de inicio de sesión.	Cumple		Se recomienda implementar los procedimientos seguros para ingresar al sistema.
9.4.3	Gestión de contraseñas de usuario.		No cumple	Se recomienda que dicha contraseña sea segura y compleja para mayor seguridad.
9.4.4	Uso de herramientas de administración de sistemas.		No cumple	Se debe controlar el uso herramientas en el sistema por uso inadecuado.
9.4.5	Control de acceso al codigo fuente de los programas.	Cumple		Todos los accesos a los códigos de fuente deben estar restringidos.
10.	CIFRADO	Cumple		La confidencialidad y la autenticidad deben estar protegidas mediante el cifrado.
10.1	Controles criptográficos.		No cumple	Se deben implementar los controles mediante políticas de seguridad.
10.1.1	Política de uso de los controles criptográficos.		No cumple	Se recomienda implementar las políticas para el uso de controles criptográficos.
10.1.2	Gestión de claves.		No cumple	Se recomienda hacer la gestión mediante la implementación de usos de llaves criptográficas durante todo el ciclo de vida.
11.	SEGURIDAD FÍSICA Y AMBIENTAL.		No cumple	Se le recomienda implementar procedimientos para prevenir cualquier tipo de interferencia de la información.
11.1	Áreas seguras.	Cumple		Se evidencia tener acceso seguro donde se encuentran los servidores.
1.1.1	Perímetro de seguridad física.	Cumple		Existe el departamento de sistema, donde están los dispositivos hardware, servidores.
11.1.2	Controles físicos de entrada.		No cumple	Se debe establecer controles para el acceso al área de sistema para mejor control.
11.1.3	Seguridad de oficinas, despachos y recursos.		No cumple	Se requiere diseñar y aplicar la seguridad al área de sistema.

11.1.4	Protección contra las amenazas externas y ambientales.		No cumple	Se debe diseñar y aplicar contra eventual desastres naturales y amenazas o ataques maliciosos.
11.1.5	El trabajo en áreas seguras.		No cumple	Se debe diseñar y aplicar procedimientos para trabajos seguros.
11.1.6	. Áreas de acceso público, carga y descarga.		No cumple	Se debe controlar los puntos de acceso tales área de despacho y de carga, despacho, y de los puntos donde pueden entrar personas no autorizadas.
11.2	Seguridad de los equipos.		No cumple	Se recomienda deben estar protegidos para reducir los riesgos de amenazas y acceso no autorizado.
11.2.1	Emplazamiento y protección de equipos.		No cumple	Se requiere mejor la protección de los equipos, instalaciones y montaje de cableado estructurado.
11.2.2	Instalaciones de suministro.	Cumple		Se evidencia que posee UPS contra fallas de fluido eléctricos que se puedan presentar.
11.2.3	Seguridad del cableado		No cumple	Se evidencia que cableado requiere una mejor protección, contra daños e interferencia.
11.2.4	Mantenimiento de los equipos.		No cumple	Los equipos presentan carencia de mantenimientos que desfavorecen la disponibilidad de los equipos.
11.2.5	Salida de activos fuera de las dependencias de la empresa.		No cumple	Debe de aplicar medidas de seguridad con los activos que se encuentran fuera de la empresa.
11.2.6	. Seguridad de los equipos y activos fuera de las instalaciones.		No cumple	De la misma manera requiere implementar medidas de seguridad cuando loa equipos salen de las instalaciones de la empresa.
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento		No cumple	Se deben verificar todos los equipos que tengan medios de almacenamientos para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o

				sobres escrito de manera segura.
11.2.8	Equipo informático de usuario desatendido.		No cumple	Requiere que los usuarios deben asegurarse que los equipos desatendidos se les den una protección apropiada.
11.2.9	. Política de puesto de trabajo despejado y bloqueo de pantalla.		No cumple	Se deben establecer unas políticas de escritorio limpio, para papeles y medios de almacenamiento removibles, y política de pantalla limpia de instalaciones
12.	SEGURIDAD EN LA OPERATIVA.			
12.1	Responsabilidades y procedimientos de operación.		No cumple	Se requiere asegurar que las operaciones sean correctas con responsabilidades y seguras.
12.1.1	Documentación de procedimientos de operación.		No cumple	Los procedimientos deben ponerse a disposición de todos los usuarios
12.1.2	Gestión de cambios.		No cumple	Se requiere controlar los cambios que se efectúen en la empresa y los sistemas de procesamientos de la información.
12.1.3	Gestión de capacidades.		No cumple	Se recomienda hacer seguimientos al uso de los recursos, como también hacerle ajustes y hacer proyecciones de los requisitos de capacidades futuras.
12.1.4	Separación de entornos de desarrollo, prueba y producción.	Cumple		Cumple con el requerimiento de separación del entorno en lo concerniente a pruebas para minimizar los riesgos.
12.2	Protección contra código malicioso.		No cumple	Asegurar que la información este protegida contra códigos maliciosos, mal intencionados.
12.2.1	Controles contra el código malicioso.		No cumple	Se recomienda implementar los controles contra el código malicioso y concientización de los usuarios.
12.3	Copias de seguridad.	Cumple		Establecer controles de copias de seguridad contra perdidas de datos. Tienen Backup.
12.3.1	Copias de seguridad de la	Cumple		Se realizan copias de seguridad de la

	información			información del software, mediante imágenes.
12.4	Registro de actividad y supervisión.		No cumple	Se recomienda registrar los eventos y dejar evidencias del mismo para un mejor control.
12.4.1	Registro y gestión de eventos de actividad.		No cumple	Se debe dejar evidencia de las actividades de registro y gestión de eventos con regularidad.
12.4.2	Protección de los registros de información.		No cumple	Se recomienda controlar los registros de la información contra una eventualidad de ataques que pueden causar daños.
. 12.4.3	Registros de actividad del administrador y operador del sistema.		No cumple	Se deben registrar las actividades del administrador y operador del sistema, como también estos registros se deben proteger y registrar.
12.4.4	Sincronización de relojes.		No cumple	Todos los registros del sistema deben ser registrados mediante una sola fuente de referencia de tiempo.
12.5	Control del software en operacional.		No cumple	Se requiere asegurarse de la integridad del software en operación, se deben tomas medidas para ello.
12.5.1	Instalación del software en sistemas en producción.	Cumple		Se evidencia que existe un procedimiento de control de software documentado en el sistema para producción
12.6	Gestión de la vulnerabilidad técnica.		No cumple	Prevenir el aprovechamiento de vulnerabilidad técnica.
12.6.1	Gestión de las vulnerabilidades técnicas.		No cumple	Se recomienda establecer un sistema de gestión de vulnerabilidad, técnica de los sistemas de información que se usen, evaluando la exposición y tomar las medidas apropiadas para tratar el riesgo
12.6.2	Restricciones en la instalación de software.		No cumple	Existen reglas para la instalación de software pero no se cumplen.
12.7	Consideraciones de las auditorías de los sistemas de			Minimizar el impacto de las auditorías sobre los sistemas operativos.

	información.			
12.7.1	Controles de auditoria de los sistemas de información.		No cumple	Los requisitos de auditorias de los controles se deben realizar cuidadosamente, planificando para minimizar las interrupciones
13.	SEGURIDAD EN LAS TELECOMUNICACIONES.			Gestión de la seguridad de redes.
13.1	Gestión de la seguridad en las redes.		No cumple	Asegurar la protección de la información de las redes y sus instalaciones de procedimientos de instalación y soporte.
13.1.1	Controles de red.		No cumple	Se requiere controlar mediante gestión para proteger la información de las redes.
13.1.2	Mecanismos de seguridad asociados a servicios en red.		No cumple	Se recomienda establecer los mecanismos de seguridad, los niveles de servicios y los requisitos de gestión de todos los servicios de la red.
13.1.3	Separación en las de redes.		No cumple	Se recomienda separar de las redes los grupos de servicios de información, usuarios y sistemas de información.
13.2	Intercambio de información con partes externas.			Mantener la seguridad transferida dentro de la organización.
13.2.1	Políticas y procedimientos de intercambio de información.		No cumple	Se recomienda implementar políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información.
13.2.2	Acuerdos de intercambio.		No cumple	Se deben implementar controles de acuerdos, para la transferencia segura entre la empresa y las partes externas.
13.2.3	Mensajería electrónica.		No cumple	Requiere proteger la mensajería electrónica se evidencia fallas en correo interno.
13.2.4	Acuerdos de confidencialidad y secreto	Cumple		Se recomienda revisar estos acuerdos y documentarlos de la confidencialidad para garantizar la protección de la información.
14.	Adquisición, desarrollo y			

	mantenimiento de los sistemas de información.			
14.1	Requisitos de seguridad de los sistemas de información.		No cumple	Asegurar que la información sea una parte integral de los sistemas de información, se deban incluir en los requisitos para un nuevo sistema de información o para mejorarlo.
14.1.1	Análisis y especificación de los requisitos de seguridad.	Cumple		Se contemplan los requisitos con la seguridad de la información, para mejorar el sistema existente
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.		No cumple	Requiere establecer el control que involucra a los servicios de aplicación que pasen por las redes públicas, protegiéndolas de actividades fraudulentas.
14.1.3	Protección de las transacciones por redes telemáticas.		No cumple	Requiere establecer el control que involucren la seguridad de la red y el cableado estructurado.
14.2	Seguridad en los procesos de desarrollo y soporte.		No cumple	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida del desarrollo del sistema de información.
14.2.1	Política de desarrollo seguro de software.		No cumple	Se deben establecer y aplicar reglas para el desarrollo de software y de sistema en la empresa ya que no la tiene.
14.2.2	Procedimientos de control de cambios en los sistemas.		No cumple	Requiere establecer controles dentro del ciclo de vida de desarrollo de software y de sistema en la empresa.
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Cumple		Aunque se efectúan pruebas para cambio de plataforma de operación se ve afectada operacionalmente.
14.2.4	Restricciones a los cambios en los paquetes de software.	Cumple		Existe una restricción para el cambio de paquetes de software.
14.2.5	Uso de principios de ingeniería		No cumple	Requiere documentar y mantener los

	en protección de sistemas.			principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de seguridad.
14.2.6	Seguridad en entornos de desarrollo.		No cumple	Requiere implementar la protección adecuadamente de ambientes de desarrollo seguro.
14.2.7	Externalización del desarrollo de software.	Cumple		El desarrollo de software se realiza externamente con seguimiento.
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Cumple		Si se realizan las pruebas de funcionalidad, para verificar su operatividad
14.2.9	Pruebas de aceptación.		No cumple	No presenta estas pruebas, se requiere implementarlas para las nuevas versiones de sistemas.
14.3	Datos de prueba.			Aceptación de los datos.
14.3.1	Protección de los datos utilizados en pruebas.	Cumple		Los datos de pruebas se protegen y se controlan cuidadosamente.
15.	RELACIONES CON SUMINISTRADORES.			
15.1	Seguridad de la información en las relaciones con suministradores.		No cumple	Se requiere asegurar la protección de los activos que sean accesibles a los proveedores.
15.1.1	Política de seguridad de la información para suministradores.		No cumple	Se requiere que la información sea segura y documentada y así mitigar los riesgos
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.		No cumple	Los requisitos se recomienda que sean acordados para fortalecer la comunicación con este.
15.1.3	Cadena de suministros de tecnología de información y		No cumple	Se requiere incluir requisitos de seguridad para tratar lo referente asociados a la

	comunicación			cadena de suministros de comunicación.
15.2	Gestión de la prestación del servicio por suministradores.			
15.2.1	Supervisión y revisión de los servicios prestados por terceros.		No cumple	Se recomienda la supervisión de los servicios realizados por terceros, revisados y auditados.
15.2.2	Gestión de cambios en los servicios prestados por terceros		No cumple	Debe gestionar los cambios de suministros por tercero, como el mantenimiento y la mejora continua dado la criticidad que tiene la información.
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
16.1	Gestión de incidentes de seguridad de la información y mejoras.			El enfoque coherente y eficaz para la gestión de los incidentes de seguridad.
16.1.1	Responsabilidades y procedimientos.		No cumple	Debe establecer las responsabilidades para la gestión eficaz y rápido de los incidente de seguridad
16.1.2	Notificación de los eventos de seguridad de la información.		No cumple	Tan pronto como ocurra el incidente de seguridad este debe ser notificado.
16.1.3	. Notificación de puntos débiles de la seguridad.		No cumple	Dado que los empleados no reportan debilidades observadas por ello es crítica.
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.		No cumple	Se videncia la no valoración y clasificación de incidentes presentados.
16.1.5	Respuesta a los incidentes de seguridad.		No cumple	No se generan respuestas de incidentes de seguridad presentados.
16.1.6	Aprendizaje de los incidentes de		No cumple	Requiere retroalimentar la información de

	seguridad de la información.			los incidentes presentados.
16.1.7	Recopilación de evidencias.		No cumple	No se lleva a cabo la recopilación de las evidencias, de incidentes presentados.
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
17.1	Continuidad de la seguridad de la información.			La continuidad de la seguridad de la información. Deben estar contenidos en la gestión de continuidad de negocio.
17.1.1	Planificación de la continuidad de la seguridad de la información.		No cumple	Se debe determinar sus requisitos para la seguridad de la información, y más aún ante eventual crisis.
17.1.2	Implantación de la continuidad de la seguridad de la información.		No cumple	Aunque es un propósito de la empresa carece de los controles necesarios para la seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		No cumple	Como carece de controles, no hay verificación de los mismos.
17.2	Redundancias.			Asegurar la disponibilidad de las instalaciones de procesamiento de la información.
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.		No cumple	Se evidencia fallas en la disponibilidad para el procesamiento de la información careciendo de redundancia.
18.	CUMPLIMIENTO.			
18.1	Cumplimiento de los requisitos legales y contractuales.			Evitar el incumplimiento de las obligaciones legales para la seguridad de la información.
18.1.1	Identificación de la legislación	Cumple		Presenta los requisitos legales, reglamentarios y contractuales de la

	aplicable.			organización.
18.1.2	Derechos de propiedad intelectual (DPI).	Cumple		Presenta el cumplimiento de los derechos legales de propiedad intelectual.
18.1.3	Protección de los registros de la organización.	Cumple		Los registros se encuentran protegidos
18.1.4	Protección de datos y privacidad de la información personal.	Cumple		Evidencia que los datos están protegidos, como lo exige en la legislación.
18.1.5	Regulación de los controles criptográficos.		No cumple	Se evidencia la necesidad es establecer los controles criptográficos.
18.2	Revisiones de la seguridad de la información.			Asegurar que la seguridad de la información se implemente y opere de acuerdo a las políticas y procedimientos organizacionales
18.2.1	Revisión independiente de la seguridad de la información.		No cumple	Se, recomienda implementar el enfoque de la empresa para la gestión de la seguridad de la información (es decir, los objetivos del control los controles y la política de seguridad)
18.2.2	Cumplimiento de las políticas y normas de seguridad.		No cumple	El compromiso de revisar con regularidad el cumplimiento de los procedimientos y procesamiento de la información por parte de la dirección.
18.2.3	Comprobación del cumplimiento.		No cumple	Se debe controlar la revisión periódica para determinar el cumplimiento con las políticas y las normas de seguridad.

Fuente el Autor

14.2 *MATERIALES NECESARIOS*

Toda documentación necesaria como sugerencia para el proceso de investigación, como las herramientas, encuestas realizas al azar a 20 empleados con sus respectivos privilegios que tienen dentro de la empresa, y plantillas de la norma ISO IEC/2001 necesarias para implementar dentro de la organización para que

nuestros objetivos vayan tomando forma de un SGSI diseñado dentro de RYMCO S.A.

De igual pondremos a consideración desde ya los pasos necesarios para las recomendaciones de este diseño de implementación de la norma ISO IEC/27001-2013

- ✓ Obtener el apoyo de la dirección
- ✓ Elaborar un plan de proyecto
- ✓ Definir el alcance del SGSI
- ✓ Redactar una Política de SGSI a nivel de la alta gerencia.
- ✓ Desarrollar las metodologías de la evaluación de riesgo.
- ✓ Realizar las evaluaciones y tratamiento de riesgo.
- ✓ Redactar la Declaración de aplicabilidad.
- ✓ Redactar el plan de tratamiento de riesgo
- ✓ Definir el método para definir la eficacia de los controles.
- ✓ Implementar los controles y procedimientos obligatorios.
- ✓ Implementar programas de capacitación y concienciación.
- ✓ Gestionar las actividades diarias del SGSI.
- ✓ controlar el funcionamiento del SGSI.
- ✓ Realizar las auditorías internas.
- ✓ Realizar la revisión por parte de la gerencia.
- ✓ Implementar todas las medidas correctivas y preventivas necesarias.

15 NORMAS Y POLÍTICA DE SEGURIDAD

15.1 ROLES Y RESPONSABILIDADES

El ingeniero de sistema es el jefe del departamento de sistema y a su vez es encargado de velar y liderar, difundir, capacitar, promover las auditorías internas, revisar los procedimientos, e impulsar por el cumplimiento de las normas y las políticas de seguridad en la empresa RYMCO S.A.

15.2 ACCESO A LA INFORMACIÓN

El personal que ingrese a laborar dentro de la empresa RYMCO S.A, recibirá capacitación y se delimitara el tipo de acceso que tendrá a la información mediante enrolamiento al sistema mediante la creación de su usuario y contraseña segura.

De igual manera está prohibido el intercambio de contraseñas, con otros miembros de la empresa. Las contraseñas para cumplir con la seguridad de esta serán asignadas por el sistema con letras mayúsculas y minúsculas, números, y caracteres necesarios para una contraseña segura. En caso de olvido de la contraseña, el trabajador se dirigirá al departamento de sistemas para restaurar o cambiar la contraseña si se requiere efectuar.

De la misma manera al terminar el contrato entre trabajador y empresa el departamento de recursos humanos enviara un mail al departamento de sistema para dar de baja, de la base de datos del sistema el acceso del trabajador retirado.

El acceso a la información en papel y la custodia del mismo solamente tendrá acceso a ella el personal autorizado, evitando que personesajena a la empresa RYMCO S.A, tenga acceso a ella.

15.3 ASPECTO RELACIONADO CON EL TRABAJADOR

El personal tras firmar un contrato laborar con RYMCO S.A, recibirá un documento de las medidas de seguridad, en donde se le recogerá su firma de recibido, en donde se le comunica lo sensible que es la información y las normas reglamentarias dentro de las misma, entre las cuales tenemos

- El personal que labora dentro de la empresa no podrá descargar música, películas u otro archivo considerados como no legales.

- Por ninguna razón el personal no podrá abrir documentos adjuntos o hacer clic a tipos de mensajes no solicitados.

- Los empleados de la organización no podrán visitar sitios web pornográfico o de contenido ilícito.

- El personal no podrá proporcionar datos personales por internet o vía mail.

- El personal de no utilizará la misma contraseña en diferentes páginas web.

- El personal de la organización no podrá instalar software sin la debida notificación al departamento de sistema, quien comprobara la legalidad del mismo.

- La información confidencial no podrá ser compartida con terceros.

- El uso de dispositivos de almacenamientos extraíbles USB está prohibido su uso dentro de la empresa.

- Quien ocasione daños al hardware, software, red recibirá la debida sanción de carácter disciplinar.

15.4 ACCESO A INTERNET

Los empleados de RYMCO S.A, no tendrán acceso a la web de internet, como a las cuentas de correos externos. Solo tendrán acceso al Intranet (correo interno de la empresa). El acceso a internet solo será concedido bajo petición de responsable jerárquico al responsable de la seguridad de la información.

15.5 SALVAGUARDA DE LOS DATOS

La persona responsables del departamento de sistema velara por la seguridad de la información, para ello garantizara la salvaguarda de los datos en soportes magnéticos u ópticos con la periódica requerida en cada caso a fin de garantizar su establecimiento en caso de incidente de seguridad.

16 PLAN DEL PROYECTO

EL diseñado este modelo de documento para la implementación del SGSI de RYMCO S.A con la información necesaria desde el código y la versión hasta la tabla de contenido necesario según la norma ISO/IEC 27001-2013.

16.1 PLAN

1. Establecer una política de la seguridad de la información
2. Dirigido a empleados, clientes, y proveedores
3. Asegurar la implementación de las medidas de seguridad comprendidas en el diseño a implementarse
4. Definir un modelo de administración de riesgos que permita un adecuado control sobre los incidentes de seguridad que puedan afectar a la empresa.
5. Proteger los activos de la información mediante procedimiento que garanticen su seguridad frente a amenazas internas o externas
6. Implementar un plan de capacitación, diseñado para generar concientización y cultura de seguridad de todos los trabajadores de la empresa
7. Proteger de forma adecuada la información para asegurar continuidad de negocio
8. Garantizar el compromiso de la dirección de la empresa para la implementación de estrategias de seguridad de información
9. Definir y administrar mediante establecimiento de rol de liderazgo el control del sistema de la seguridad de la información
10. Cumplimiento de las normas legales vigente que garanticen la seguridad de la información de la empresa.

16.2 FORMATO DEL PLAN

Plan para la implementación de un Sistema de gestión de Seguridad de la información (SGSI) en el área de sistema bajo la norma ISO 27001-2013. (Ver Anexo 1, Ver Anexo 2 y Ver Anexo 3)

Código	24
Versión:	1
Fecha de la versión:	MAYO 7 2015
Creado por:	Pedro Samperl
Aprobado por:	Ricardo Escalante
Nivel de confidencialidad:	Alto

Fuente el Autor

16.3 PARA LA PROPUESTA DISEÑADA DEL SGSI SON NECESARIOS LOS SIGUIENTES ANEXOS IEC/27001-2013

1. Organización de la seguridad de la información.
    - Políticas de dispositivos.
2. Seguridad relacionada con el personal.
    - declaración de aceptación de documento.
3. Gestión de activos
    - inventario de los activos.
4. Control de acceso.
    - políticas de claves.
5. Criptografía.
    - Políticas de controles criptográficos.
6. Seguridad física ambiental.
    - Políticas para trabajo en áreas.
7. Seguridad operativa.
    - Políticas de creación de copias de seguridad.
8. Seguridad de las comunicaciones.
    - Políticas de transferencia de información.
9. Adquisición y desarrollo de mantenimiento.
    - Políticas de desarrollo seguro.
10. Relaciones con proveedores.
    - Políticas de seguridad con proveedores.
11. Gestión de los incidentes de seguridad.
    - Procedimientos para gestión de incidentes.

Fuentes La academia ISO 27001

16.4 PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN DEL ÁREA DE SISTEMA

Con el objetivo de preparar al personal del área de sistema para que pueda cumplir una función en la seguridad de la información, se debe llevar a cabo un plan de capacitación con los siguientes lineamientos.(Ver Anexo 5)

16.5 LISTA DE VERIFICACIÓN DEL DISEÑO DE SGSI PARA IMPLEMENTACIÓN DE ISO 27001:2013

(Ver Anexo 6)

16.6 ENCUESTA

La encuesta se realizó solo el personal de distintas áreas de la empresa, incluyendo a la única persona del área de sistema dado que el alcance de nuestro proyecto está orientado hacia área de sistema de la empresa RYMCO S.A.

El personal encuestado corresponde solamente al personal que se encontraba trabajando en el turno de día entre la 08:00 am hasta las 16:00 pm. Números de empleados encuestados 20 totales. (Ver Anexo 7)

16.7 *RECURSO Y PRESUPUESTO*

Los recursos y presupuestos representan la inversión y el compromiso de la gerencia para el desarrollo del proyecto de carácter investigativo para el diseño del sistema de gestión de la seguridad informática en el área de sistema. (Ver Anexo 8)

16.8 *CRONOGRAMA*

El siguiente cronograma representa el itinerario del desarrollo para el inicio y culminación de esta propuesta de proyecto de un diseño de un SGSI en el área de sistemas de la empresa RYMCO S.A bajo la norma ISO IEC/27001:2013. (Ver Anexo 9)

17 CONCLUSIONES

Mencionamos antes que la seguridad de la información se encarga de protegerla, más específicamente, podemos definir que lo logrará preservando la confidencialidad, integridad y disponibilidad de la información, como aspectos fundamentales y el control y autenticidad como aspectos secundarios . A continuación se describen estas características:

- ✓ La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

- ✓ La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

- ✓ La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

- ✓ El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

- ✓ La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades. Adicional mente pueden considerarse algunos otros aspectos, relacionados con los anteriores, pero que incorporan algunas consideraciones particulares:

- ✓ Protección a la Réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

- ✓ No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

Es fundamental, que mediante el concepto de mejora continua, favorecerá en la empresa la consecución de los objetivos esperados y el fortalecimiento para la continuidad de negocio razón de ser de este diseño de proyecto para un SGSI en el área de sistema de la empresa RYMCO S.A. El enfoque sistemático propuesto por la norma ISO/IEC 27001:20013 permitirá las siguientes consecuencias:

- ✓ La toma de decisiones sobre la seguridad de los activos críticos de la información se basa en información a priori (análisis de riesgos) y a posteriori (auditorio e indicador).

- ✓ Se orienta a la mejora continua, a través de la gestión de acciones correctivas y preventivas.

- ✓ Si se decide obtener la certificación ISO/IEC 27001:2013 del sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los usuarios y RYMCO S.A.

En sintaxis toda organización como RYMCO S.A tiene como objetivos primordial el, fortalecimiento de sus productos en el mercado y los negocios, y requiere que desde los procesos de operaciones de fabricación de sus productos hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable. Si bien es cierto que gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, y aquí entra en juego un SGSI.

La empresa RYMCO S.A y al igual que cualquier otra empresa que no fortalezca sus procesos operativos en harás de salvaguardar sus activos, decaerá, su principal aliado son los clientes y si este no se encuentra a gusto con su proveedor, simplemente lo que hace es buscar otro proveedor que si le garantice satisfacción total que este desea. La implementación de un SGSI, disminuyen el impacto, en cuanto a los riesgos potenciales que está expuesto, sin la necesidad de implementar grandes cambios, los controles cuanto se establecen logramos mantener los riesgos y amenazas en un nivel controlable. Finalmente no está decir de más las bondades que nos proporcionan las normas ISO IEC/27001-2013.

RECOMENDACIONES

Que es este diseño metodológico de este proyecto represente a la empresa RYMCO S.A el conjunto de directrices necesarias para la implementación de un SGSI, y logre fortalecer su funcionamiento en el mercado como empresa líder en la fabricación de sus productos. El siguiente paso es la certificación ante la norma ISO IEC/27001:2013. En este proyecto mencionamos los 16 pasos para la consecución del objetivo, con su debida evidencia que lo demuestren.

La empresa debe fortalecer el departamento de sistema.

La empresa puede contar con auditores internos de la misma empresa, pero previamente capacitados para tal fin.

Nuestro objetivo final es fortalecer el AREA DE SISTEMA dado que en este está orientado nuestro proyecto en harás de promover su implementación la mejora continua logrando el fortalecimiento de su seguridad y la confianza de sus clientes.

Finalmente dentro de las recomendaciones la más importante de todas, es que conocido este modelo diseño de SGSI para RYMCO S.A en aras de conseguir que objetivos planteados en este proyecto sean de apoyo para la implementación futura y puesta en marcha para obtener la certificación del SGSI ISO/IEC 27001-2013

BIBLIOGRAFIA

Articulo Web.

WIKIPEDIA LA ENCICLIPEDIA LIBRE "Sistema de gestión de la seguridad de la información: [3 de septiembre 2012 Disponible en: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

ARTICULO DE INERNET

Articulo web

JOHANNA CAROLINA BUITRAGO ¨Sistema de gestión de la seguridad de la [Bogotá 2012 Disponible en en.información¨.http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

Artículo web.

CREATIVE COMMONS ATRIBUTION-SHARE "Seguridad de información Octubre de 2012 Disponible en "http://190.90.112.209/http/criptografia/Seguridad_de_la_informacion.pdf

Artículo web.

CREATIVE COMMONS ATRIBUTION-SHARE "Seguridad de información Octubre de 2012 Disponible en "http://190.90.112.209/http/criptografia/Seguridad_de_la_informacion.pdf

UNIVERSIDAD LIBRE ""La información es un poder" Bogotá 2015] Disponible el

http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

Artículo web.

NORBERTO MORENO WORDPRESS. "Que es seguridad de la información" Abril de 2014. Disponible en

https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdf

Artículo web.

ANGIE GARZON- "Que es el ciclo PHVA" [Noviembre de 2013] Disponible en http://es.scribd.com/doc/96330540/ciclo-PHVA

Artículo web.

SEMINARIO ISO .“Norma ISO IEC/27001” Disponible en http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

Artículo web.

CIBERSEGURIDAD. “Herramienta de análisis de gestión de riesgo”. Septiembre de 2014. Disponible en https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

Artículo web.
CDN-ISO 27001 STANDARD. Lista de documentos obligatorios requeridos norma ISO IEC/27001:2013 Disponible en http://cdn2.iso27001standard.com/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013_ES.pdf

Artículo web.
KRIPTOPOLIS “Dirección web criptografía y seguridad Kriptopolis, 1996 2014 “Disponible en http://www.kriptopolis.com/
PROMOTEC S.A., Sede Principal Av. Caracas No. 28A-17 Bogotá D.C. Recomendaciones de seguridad informática

Artículo web.
PROMITEC WEB- “Recomendaciones de la seguridad informática” 2014 Disponible en http://www.promotec.com.co/WebSite/Contenido.aspx?ID=RecomendacionDeSeguridadInformatica

Artículo web.
MUNDONETS WEB. “Presentación de trabajos escritos Norma NCT 1486” 2014- Disponible en http://www.mundonets.com/normas-icontec/

Libro
CONSTAIN MORENO Gustavo Eduardo, RAMIREZ VILLEGAS Gabriel Mauricio. Modulo modelo y estándares de seguridad informática: UNAD (2013: Santafé de Bogotá), recuperado 28 Agosto de 2011

Libro
Normas APA para trabajos escritos y documentos de investigación. Bibiana del Carmen Ávila_ UNAD.2013

Módulo de Proyecto de Seguridad Informática 1. Esther Angélica Sabogal Rozo_ Universidad Abierta y a Distancia_UNAD. 2013_II

Libro

SEGURITY & BUSINESS CONTINUITY ACADEMY Diagrama del proceso de implementación de la norma 27001**:2013**.http://www.iso27001standard.com/es

Libro

BETARTE, Gustavo, CORTI María Eugenia, DE LA FUENTES Reinaldo. Hacia un. (2014 Santa fe de Bogotá). Pdf.dto.

ANEXOS

Anexo 1. Plan de auditorías internas

RYMCO	PLAN DE AUDITORIAS INTERNAS	CODIGO FOR-AUD-006 VERSIÓN 1 PAG 1 DE 1

AUDITORIA N°		Norma de referencia		Fecha de elaboración
ALCANCE				
OBJETIVOS				
Auditor líder				
Auditores interno				
Expertos técnicos				
Observadores				

Fecha	Hora	Area/Proceso a auditar	Criterio del auditor		Auditor	Auditado
			Clausula a auditar	Documentación		
REUNION DE APERTURA			REUNION DE CIERRE			

Fecha	Hora		Fecha	Hora	

Fuentes: el autor

Anexo 2. Informe de auditoría internas/formato

RYMCO	**INFORME DE AUDITORIAS INTERNAS**	CODIGO FOR-AUD-007 VERSION 1 PAG 1 DE 1

1. DATOS DE LA AUDITORIA INTERNA

Auditoria N°	
Norma de referencia	
Periodo de la auditoria	
Lugar de la auditoria	
Equipo auditor	

2. ALCANCE DE LA AUDITORIA

2.1. EXCLUSIONES REPORTADAS:

3. OBJETIVO DE LA AUDITORIA

- Determinar el grado en cual el SGSI cumple con los requisitos de la norma ISO IEC/27001:2013

4. DEDINICIONES

4.1. NO CONFORMIDAD.

4.2. OBSERVACIONES.

4.3. OPORTUNIDAD DE MEJORAS.

5. FORTALEZAS Y DEBILIDADES

FORTALEZAS	DEBILIDADES
• A	• A

• B	• B

6. RESULTADO DE LA AUDITORIA

6.1. NO CONFORMIDADES:

Se hallaron_____No conformidades NC durante la auditoria interna. Las no conformidades se resumen en el siguiente cuadro.

AREA/PROCESO	SAC	DESCRIPCION	RESPONSABLE	AUDITOR

6.2. OBSERVACIONES Y OPORTUNIDADES DE MEJORAS:

Las observaciones (OBS) y oportunidades (OM) de mejoras identificadas durante la auditoria interna

- A
- B

7. CONCLUSIONES DE LAS AUDITORIAS INTERNAS

- A
- B

Anexo 3. Solicitud de acción/formato.

RYMCO	SOLICITUD DE ACCION	CODIGO FOR-AUD-008 VERSION 1 PAG 1 DE 1

SOLICITUD N°		NORMA REFERENCIA	

Acciones Preventivas	Acciones Correctivas	Servicio No conforme

Hallazgo	Auditoria	Reclamo del cliente	Revisión por la dirección	Análisis de datos	Observaciones del personal

I. DESCRIPCIÓN

Informado por:	

Responsable :		Fecha	

II. ANALISIS DE CAUSAS

Responsable:		Fecha	

III. ACCIONES A TOMAR

1. Acciones Inmediata o Corrección (solo para los casos que aplique)

2. Acción Preventiva/Correctiva (Plan de acción)

N°	Actividad	Responsable	Tiempo

Responsable		Fecha	
Fecha de cierre de propuesta			
IV. VERIFICACION			
CONFORME		NO CONFORME	
RESPONSABLE		FECHA DE CIERRE REAL	

Fuentes el Autor

Anexo 4. Formato plan de capacitación

Cargo o nombre	*Que capacitacion es necesaria*	*Lugar y fecha de la capacitación*	*Control de evaluaciones relevante a la capacitación*	*Responsable de la capacitación*

Fuentes: el Autor

Anexo 5. Formato lista de verificación del diseño de SGSI

Fases de implementación	Tareas	Terminado
Obtener el apoyo de la dirección	Investigar qué beneficios de ISO 27001 serían aplicables a su empresa	
	Presentar los beneficios a la dirección y obtener su compromiso	
	Obtener la aprobación formal para el proyecto	
Prepararse para su proyecto	Decidir si va a utilizar consultores o si utilizara plantillas de documentación	
	Comprar la norma ISO 27001	
	Capacitar a su equipo para el proyecto	
	Escribir el plan del proyecto, incluyendo la definición del gerente del proyecto, equipo del proyecto, promotor del proyecto, recursos necesarios y objetivos parciales	
	Definir qué partes interesadas necesitan estar informadas sobre cada paso del proyecto	
	Organizar reunión inicial	
Identificar los requerimientos	Identificar las partes interesadas	
	Identificar los requisitos de las partes interesadas	
Definir el alcance , la intención y las responsabilidades de la dirección	Redactar el documento de alcance del SGSI	
	Redactar la Política de seguridad de la información	
	Decidir los objetivos de seguridad de la información	

Implementar procedimientos de apoyo	Redactar procedimiento para control de documentos	
	Redactar procedimiento para auditoría interna	
	Redactar procedimiento para medidas correctivas	
Realizar gestión de riesgos	Desarrollar la metodología de evaluación de riesgos	
	Realizar evaluación de riesgos	
	Realizar tratamiento de riesgos	
	Redactar el informe sobre evaluación y tratamiento de riesgos	
Desarrollar el perfil de seguridad de su empresa, el plan de acción y cómo ejecutarlo	Desarrollar la Declaración de aplicabilidad	
	Desarrollar el Plan de tratamiento de riesgos	
	Aceptar los riesgos residuales	
Implementar los controles	Implementar todos los controles definidos en el Plan de tratamiento de riesgos	
	Mantener registros de implementación	
Realizar programas de capacitación y concienciación	Realizar la capacitación para todos los empleados que carecen de las habilidades necesarias	
	Ejecutar programas de concienciación para todos los empleados y terceros que cumplen una función en su SGSI	
Hacer funcionar el SGSI	Mantener todos los registros requeridos por sus propias políticas y	

	procedimientos	
	Aplicar medidas correctivas según sea necesario	
Supervisar y medir el SGSI	Asegúrese de supervisar todos sus sistemas	
	Medir si ha alcanzado los objetivos fijados para su SGSI y para sus controles	
Realizar la auditoría interna	Desarrollar el programa de auditoría	
	Realizar la(s) auditoría(s) interna(s)	
	Redactar un informe de auditoría interna	
	Aplicar medidas correctivas	
Realizar la revisión por parte de la dirección	Realizar la revisión por parte de la dirección	
	Guardar registros de la revisión por parte de la dirección	
	Aplicar medidas correctivas	
Auditoría de certificación	Obtener propuestas de varias entidades de certificación	
	Elegir la entidad de certificación	
	Fase 1 de auditoría de certificación	
	Fase 2 de auditoría de certificación	
	Visitas de supervisión	

Fuente el Autor

Anexo 6. Formato de encuesta

ENCUESTA

EMPRESA	RYMCO S.A	SECCION	
CARGO		TELEFONO	
FECHA		CELULAR	

INTRUCCIONES

Responda la siguiente encuesta, de aspecto relacionado con la seguridad de la empresa.

Parte1. **Pilares de la seguridad** disponibilidad, desempeño, confidencialidad, integridad, control a acceso físico y lógico.

Comente sobre ellos.

1. Considera importante la seguridad informática en la empresa:

a) SI	
b) NO	
c) NINGUNA	

2. Tiene acceso a todo el sistema de la empresa.

a) SI	
b) NO	
c) Casi todo	

3. Que reporta en el sistema.

a) Datos	
b) Informes/datos	
c) Navega en internet	

4. Describa que tipos de componentes hardware plano existen en la empresa.

a) router	
b) impresoras	
c) escáner	
d) swtch	

Parte 2 **Capacitación**

1. Describa las capacitaciones que recibe de sistemas:

a) Seguridad	
b) Uso de contraseña	
c) Manejo de sistemas	
d) Otros	

2. Conoce de sistemas.

a) Lo requerido	
b) No lo manejo	
c) Requiero capacitación	
d) Con conocimiento	

3. En qué nivel educativo está usted

a) bachiller	

b) técnico	
c) profesional	
d) Tecnólogo	

4. Herramientas informáticas que maneja dentro de la empresa.

a) CPU /escaner/impresora	
b) Tablet/ CPU	
c) Fax / impresora/ CPU	
d) Todas las anteriores	

Fuente el Autor

Anexo 7. Resultados de la encuesta

RESULTADO DE LA ENCUESTA REALIZADO A 20 EMPLEADOS DE TODAS LAS AREA DE LA EMPRESA																					
Empleado	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	total
Capacitación																					
Seguridad														1							01
contraseña	X		X	X			X	X	X		X		X		X	X			X	X	12
manejo	X	X		X	X		X	X	X		X		X		X	X		X	X	X	14
otros																					00
Conoce de sistema																					
Requerido		X	X	X	X	X	X	X				X		X	X	X		X	X	X	15
No conozco	X								X	X	X		X				X				06
Requiero capacitación	X								X	X	X		X				X				06
Conozco Bien	X												X				X				03
Nivel de educación																					
Bachiller	X	X	X	X													X	X			06
Técnico					X	X	X	X	X	X									X	X	08
Tecnólogo											X	X	X								03
Profesional														X	X	X					03
Que reporta																					

Datos			X	X																	02
Informe/Datos	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	18
Navega en internet															X	X	X				03
TOTAL DE DATOS																					100
OBSERVACIONES: Nótese que la única persona que contesto seguridad, es la única del área de sistema																					

Fuentes el Autor

Anexo 8. Recursos y presupuestos

RECURSOS Y PRESUPUESTOS				
ITEM	**Actividades y otros costes Actividades y otros costes**	Recursos del régimen administrativo RYMCO CE	Compromiso especifico	TOTAL
1	**Actividades (otros)**	$ 500.000,00		
2	Actividad 1		$ 500.000,00	$ 500.000,00
3	Actividad 2		$ 4.000.000,00	$ 4.000.000,00
4	Actividad 3		$ 1.500.000,00	$ 1.500.000,00
5	SUBTOTAL			
6	INVERSIONES			
7	Equipos	$ 3.000.000,00		
8	Transporte	$ 500.000,00		
9	Material	$ 500.000,00		
10	SUBTOTAL	$ 4.000.000,00		
11	Funcionamiento			
12	Otros Gastos	$ 500.000,00		
13	alquiler oficina	$ 1.000.000,00		
14	SUBTOTAL	$ 1.500.000,00		
	TOTAL			$ 6.000.000,00

Fuentes el Autor

Anexo 9. Cronograma del proyecto

CRONOGRAMA												
PROYECTO DE DISEÑO DE UN SGSI EN RYMCO S.A												
Actividades por semanas	2014				2015				ENTREGA SEMANA			JUNIO
	OCT	NOV	DIC		FEB	MAR	ABR	MAY	1	2	3	4
Propuesta plan de diseño	●	●	●									
Recopilación de la información					●	●						
Análisis de riesgo						●	●					
Desarrollo del proyecto							●	●	●			

Fuentes el Autor