UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:
ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN EL CRITERIO DE LA NORMA NTE INEN-ISO/IEC 27001:2011, DE UN MODELO DE NEGOCIO APLICADO EN LA COMERCIALIZACIÓN Y DISTRIBUCIÓN DE PRODUCTOS QUÍMICOS.

AUTOR:
XAVIER ALEJANDRO AGUILA PLAZA

DIRECTORA:
ING. BERTHA ALICE NARANJO

Guayaquil, marzo del 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO.

Yo Xavier Alejandro Aguila Plaza autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad el autor.

Atentamente,

Guayaquil, marzo del 2015.

Xavier Alejandro Aguila Plaza

CC: 0925188443.

AGRADECIMIENTOS.

Deseo expresar mi profunda gratitud a quienes directa o indirectamente colaboraron con el desarrollo del presente trabajo, entre ellos.

- A cada uno de los docentes que aportó a través de nuestros años de estudio, valiosos conocimientos que fomentaron nuestra capacidad y experiencia.

- A la Ing. Alice Naranjo, director de tesis, por la colaboración y asistencia constante durante el desarrollo de este trabajo de tesis

- A mis abuelos, quien con el apoyo constante y circunstancial en todo momento fue apoyo importante para seguir con este proyecto de vida.

ÍNDICE

ÍNDICE DE ANEXOS.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

RESUMEN

La importancia en la evolución y utilización de las Tecnologías de información y comunicación (TICs) ha incidido mucho en el desarrollo de las organizaciones, obligando a estas a seguir normas y estándares basado en ITIL, Cobit e ISO para poder estar a la par de los avances de las tecnologías de telecomunicaciones.

Éste proyecto de investigación va a ser de gran relevancia dentro de las organizaciones dedicadas a la comercialización y distribución de productos químicos, debido a que su principal objetivo es convertirse en lineamiento para lograr la gestión de la seguridad de la información de manera óptima y correcta.

La adopción de un SGSI (Sistema de Gestión de Seguridad de Información) basado en la norma homologada para Ecuador NTE INEN-ISO/IEC 27001:2011 ha despertado interés en organizaciones que se dedican a la comercialización y distribución de productos químicos, con la finalidad mejorar la gestión de la seguridad de información, en sus procesos y la gestión de riesgo en sus activos de información.

Los beneficios otorgados por el análisis y diseño del SGSI fueron la disminución de riesgo de los activos de la organización y el uso correcto de recursos de tecnología de información (TI) manteniendo la disponibilidad, integridad y confidencialidad de la información.

ABSTRACT

The importance of the evolution and use of the technologies for the information and communication has affected deeply in the development of the organizations, forcing them to follow ITIL, COBIT and ISO standards to be up to par with the advances in communications technologies.

This project will be of great importance within the organizations involved in the marketing and distribution of chemicals products, because the main objective is to become a guideline for the management of the information security proper and optimal.

The adoption of an SGSI based in the regulations for Ecuador NTE INEN ISO/IEC 27001:2011 have created interest in organizations dedicated to the distribution and commercialization of chemicals products with the aim of improving the management of information security in its processes, and the management of risks in its information assets.

The benefits granted due to the analysis and design of the SGSI were the diminishing of risks in the organization assets and the correct use of resources of information technologies, maintaining the availability, integrity and confidentiality of information.

INTRODUCCIÓN.

La información es el activo más crítico dentro de las organizaciones, hoy en día se puede observar en los medios de comunicación aparecer nuevos y diversos tipos de ataques informáticos, cada vez más sofisticados y con un mayor alcance. Por lo general son auspiciados por diversas fuentes, tales como gobiernos o por agrupaciones dedicadas a la piratería informática, estos actos pueden ser realizados para diversos fines tales como espionaje, extorsión, así como también pueden tener un fin de protesta o desafío personal.

Por ésta razón se ha realizado éste proyecto de investigación, con el objetivo de llegar a obtener los lineamientos necesarios para el cumplimiento de los principios de la seguridad de la información, los cuales son la integridad, disponibilidad y confidencialidad, tomando como referencia los criterios de la norma técnica NTE INEN-ISO/IEC 27001:2011, de tal manera que esté pueda ser aceptado y reconocido de manera nacional e internacional.

El presente proyecto de investigación se encuentra elaborado en seis capítulos, los cuales se detallan a continuación.

Capítulo 1: Planteamiento del problema.

En éste capítulo se ha definido los objetivos el que se ha planteado este proyecto de investigación, sus factores estructurales, intermedios e inmediatos, se presenta además el problema con su respectiva justificación, así como todos aquellos que se encontrarán favorecidos por medio de éste proyecto de investigación.

Capítulo 2: Marco Teórico.

Está compuesto por el marco teórico y el marco normativo de este proyecto de investigación, así como la formulación de la hipótesis y el señalamiento de las variables.

Capítulo 3: Marco Metodológico.

Contiene el marco metodológico, el cual muestra la modalidad de la investigación que se ha llevado para este proyecto de investigación, los métodos de la investigación que se han utilizado, los instrumentos de recolección de datos, la población y muestra y la operacionalización de las variables.

Capítulo 4: Análisis y Resultados.

Se encuentra compuesto por el análisis de las encuestas realizadas según la población y muestra anteriormente ya definida, así como la interpretación de los datos y la verificación de la hipótesis.

Capítulo 5: Propuesta.

En este capítulo se encuentra el desarrollo de los antecedentes de la propuesta, la justificación, los objetivos, el análisis de factibilidad, la fundamentación y el modelo operativo, la metodología utilizada y la administración de la misma.

Capítulo 6: Conclusiones y Recomendaciones.

Contiene las conclusiones y recomendaciones que deben de ser aplicadas para la realización de este proyecto de investigación.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. Enunciado del problema.

1.1.1. Factores Estructurales - causas.

El modelo de negocio aplicado a este estudio se encuentra orientado a la comercialización y distribución de productos químicos, por lo general estas organizaciones constantemente se encuentran en proceso de evaluación ya que siempre buscan que sus procesos de gestión alcancen niveles diferenciales en el mercado.

El mantenimiento de la seguridad de información es un factor fundamental, ya que éste garantiza que exista la disponibilidad, integridad y confiabilidad de los activos informáticos dentro de las organizaciones. Sin embargo muchos presentan riesgos determinados por diversas causas, entre ellas.

- Falencias en la correcta identificación de las vulnerabilidades y riesgos en la organización.
- Insuficiencia de manuales de funciones y procedimientos.
- Falta de políticas internas y controles aplicados como indica la norma.
- Insuficiencia de controles implementados para poder brindar protección a los activos.
- Desconocimiento y falta de concientización interna de la seguridad de la Información.
- Ausencia de revisiones constantes de carácter interno de parte del área de Dirección y Auditoría.

1.1.2. Factores Intermedios – Rasgos del Problema.

La carencia de mecanismos de seguridad degeneran en amenazas que pueden llegar a afectar a una organización en diversos aspectos, tales como:

- Política y procedimientos de seguridad.
- Análisis y Gestión de Riesgos.
- Controles de seguridad.
- Planes de Acción correctivas y preventivas.
- Procedimientos y mecanismos de control.

Como resultado de esto, se producen falencias en la gestión de la seguridad de la información.

1.1.3. Factores Inmediatos – Consecuencias.

Las consecuencias más notables por falta de seguridad son:

- Alteración de la información.
- Robo de la información.
- Perdida de la Información.
- Falta de disponibilidad en la información.
- Vulnerabilidades y riesgos en los sistemas que afectan a la integridad y confidencialidad de la información.

1.2. Formulación del Problema.

La carencia de mecanismos óptimos degenera en amenazas que pueden llegar a afectar una organización.

1.2.1. Pregunta Científica.

¿Cómo se puede establecer los niveles apropiados de integridad, disponibilidad y confidencialidad de la información en un modelo de negocio dedicado a la comercialización y distribución de productos Químicos?

1.2.2. Sistematización del problema (Preguntas Específicas).

i. ¿Qué criterios, normas o estándares de seguridad se deben aplicar en un modelo de negocio para mantener niveles de integridad, confidencialidad y disponibilidad de la información?

ii. ¿Qué elementos inciden en la falta de seguridad de la información en la organización?

iii. ¿De qué manera se pueden mitigar las vulnerabilidades que afecten la seguridad de la información?

iv. ¿De qué manera se pueden mitigar los riesgos existentes que afecten a la seguridad de la información?

1.3. Objetivos de la Investigación.

1.3.1. Objetivos Generales

Analizar y diseñar los documentos principales de un Sistema de Gestión de la Seguridad de la Información basado en el apartado **4.3.1** del criterio de la norma NTE INEN-ISO/IEC 27001:2011, para lograr garantizar niveles apropiados de integridad, disponibilidad y confidencialidad en un modelo de negocio dedicado a la comercialización y distribución de productos Químicos.

1.3.2. Objetivos Específicos

i. Desarrollar el manual del Sistema de Gestión de Seguridad de la Información, basado en el criterio de la norma INEN NTE-ISO/IEC 27001:2001, para mantener niveles de integridad, confidencialidad y disponibilidad de la información.

ii. Formular la política de seguridad estándar, según el apartado 4.3.1a) de la norma para lograr la ejecución de los procesos de manera óptima y segura.

iii. Plantear el alcance del SGSI, según el apartado 4.3.1b) de la norma.

iv. Elaborar la declaración de aplicabilidad estándar, según el apartado 4.3.1j) , para garantizar la seguridad de la información

v. Establecer una descripción de la metodología de evaluación de riesgo y el plan de tratamiento de riesgos estándar, según el apartado 4.3.1d) y 4.3.1e) de la norma

1.4. Justificación del Problema.

El no contar con mecanismos de seguridad apropiados podría ocasionar serios problemas a las organizaciones tales como:

- ✓ Falta de credibilidad con otras organizaciones.
- ✓ Pérdida de prestigio en el mercado.
- ✓ Afectación a la imagen corporativa de la empresa.
- ✓ Pérdida de fondos patrimoniales de la organización (datos, programas, información confidencial, etc.).
- ✓ Gastos financieros ocasionados por incidentes de seguridad.
- ✓ Falencias en la continuidad del negocio.
- ✓ Ausencia de nuevas oportunidades de mercado.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes Teóricos

Con el crecimiento y evolución de las organizaciones, la planificación, administración y control de los procesos se vuelve una tarea cada vez más compleja, y en el caso del manejo de los procesos de información, que es un intangible de naturaleza muy sensible, lo es más aún. En el mundo moderno, el activo más importante de una organización, después de los recursos humano, y tal vez antes que ellos, es el de la información. La información, desde el punto de vista de activo organizacional, debe ser tratada con la importancia que se merece. Con este antecedente, mientras mayor el volumen de información, se torna más necesario aplicar los conceptos de seguridad de la información, que permitan alcanzar los niveles deseados de integridad, disponibilidad y confiabilidad.

A continuación, se revisarán los conceptos más relevantes en cuanto al control y supervisión de calidad.

CSI/FBI Computer Security Crime Survey 2013.

Computer Crime Institute, es una organización internacional que realiza el estudio y el análisis de la información obtenida por la comunidad informática en los Estados Unidos de América, respecto a cómo están siendo afectadas las infraestructuras y los medios tecnológicos en las organizaciones por crímenes que afectan directamente a la seguridad de la información, a continuación se muestra el siguiente análisis estadístico respecto a los crímenes tecnológicos realizado por **CSI/FBI.**

En la figura 1 se ilustra de manera detallada los sectores de las empresas que han sufrido ataques informáticos. Acorde al documento 2013 Cyber Crime and Security Survey emitido por *Australia's national computer emergency response team, CERT Australia (the CERT)*.

Defensa	23%
Energia	16%
Financiero	13%
Gobierno	12%
Químico	11%
Manufactura	5%
Comunicaciones	5%
Recursos Mineros	4%
Transporte	3%
Salud	2%
Retails	1%

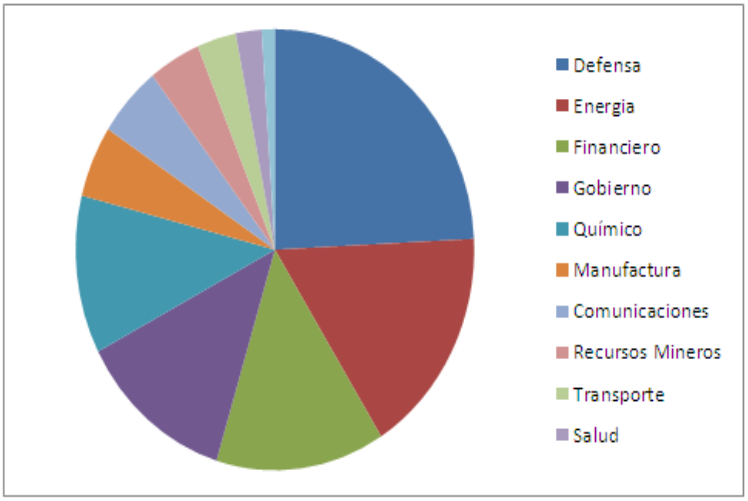


Figura 1: Actividades que desempeñan las organizaciones consultadas.

Fuente: (CERT Australia, 2013)

Del análisis realizado se ha obtenido información de suma relevancia, el cual corresponde al número de incidencias reportadas anualmente, las cuales se detalla a continuación:

- 63% - Ataques vía correo electrónico
- 52% - Infección de virus o gusanos.
- 46% - Infección de puertas traseras y troyanos.
- 35% - Amenazas a dispositivos móviles.
- 26% - Accesos no autorizados
- 17% - Extorciones.
- 17% - Denegación de servicio distribuidos.

Estas incidencias afectaron a organizaciones que contaban con herramientas para la protección de la seguridad de la información, generando considerables pérdidas en las organizaciones, por lo cual demuestra que no es suficiente poseer una gran cantidad de soluciones de seguridad o estar a la vanguardia de las soluciones de seguridad tecnológica disponibles en el mercado para llegar a obtener la disponibilidad, integridad y confiabilidad de la información.

La gestión correcta de la seguridad de la información se enfoca específicamente en un conjunto de estándares y procedimientos que involucran a todos los miembros de la organización tanto externos como proveedores y clientes así como internos que sería todos los departamentos que se encuentran dentro de la organización.

Por medio de un Sistema de Gestión de Seguridad de la Información la organización llega al punto de conocer los riesgos tanto externos como internos a los que se encuentra expuesto y como su información puede llegar a verse comprometida, de esta forma puede lograr mitigar estos riesgos y mantenerlos en un nivel aceptable a través una gestión definida y documentada.

2.2. Investigaciones previas.

Seguridad

"El término seguridad (del latín securitas) cotidianamente se puede referir a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia" (Diccionario de la Lengua Española, 2010).

Por lo tanto acorde a lo expresado anteriormente se puede indicar que la seguridad se puede referir como un bien el cual percibe y disfruta un ser humano y ésta puede ser aplicada a todas las áreas o campos en los que se desee emplear.

Tipos de Seguridad.

Los tipos de seguridad son:

- Seguridad Informática.
- Seguridad de la Información.
- Seguridad Activa.
- Seguridad Pasiva.

Seguridad Informática.

"Conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo" (García & Alegre, 2011).

"La seguridad informática se enfoca en la protección y la privatización de sus sistemas" (Ochoa Ovalles S. y Cervantes Sánchez, 2012).

Por lo tanto, la seguridad informática son todos los controles necesarios que se deben de aplicar para poder obtener niveles protección adecuados para garantizar la seguridad de los recursos tecnológicos.

Seguridad de la información.

"Disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios" (Alegsa, 2010).

"El conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma." (Lemus, 2014).

Por lo tanto se puede exponer que la seguridad de la información es la aplicación de un conjunto de regulaciones las cuales son implantadas con el objetivo de proteger la información, y de la misma manera garantizar la existencia de niveles apropiados de confidencialidad, disponibilidad y confidencialidad.

Seguridad Activa.

"El nivel de seguridad activa de un sistema en la protección antes posible intentos de comprometer los componentes que los integran un Firewall por ejemplo la seguridad activa filtra el acceso a ciertos servicios en determinados conexiones para bloquear el intento de ataque desde algún de ellos." (Ochoa Ovalles S. y Cervantes Sánchez, 2012)

Acorde a lo indicado anteriormente se puede exponer que la seguridad activa son todos los controles que se encuentran aplicados para evitar que por medio de un evento se seguridad se puede comprometer un recurso de la organización.

Seguridad Pasiva.

“Conjunto de medidas implementadas en los sistemas las cuales alerten a los administradores sobre incidentes que comprometan la seguridad " (Ochoa Ovalles S. y Cervantes Sánchez, 2012).

De lo indicado anteriormente se puede concluir que la seguridad pasiva son todos los mecanismos o regulaciones tomadas en los sistemas que se encuentran implantados dentro de una organización con el objetivo de que estos puedan alertar a los operadores o al personal del área tecnológica que un recurso informático ha sido comprometido.

Principios de la seguridad de la información.

“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.”, (Lemus, 2014).

Integridad.

"La propiedad por el que un componente de un sistema, un sistema de información o información no se haya modificado o destruido de manera no autorizada" (NICCS, 2015)

“……, es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.” (Lemus, 2014)

Por lo tanto, acorde a lo indicado anteriormente se puede exponer que la integridad de la información es el proceso por el cual la información puede ser accedida por un medio, sea este físico o lógico y no sea modificada.

Disponibilidad.

"La propiedad de ser accesible y utilizable cuando se lo demande." (NICCS, 2015)

"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. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran" (Lemus, 2014)

Por lo tanto, acorde a lo indicado anteriormente se puede exponer que se refiere a disponibilidad el acceso de un recurso informático cuando este se lo requiera.

Confidencialidad.

"La propiedad de que no se divulga información a los usuarios, procesos o dispositivos a menos que ellos hayan sido autorizados a acceder a la información" (NICCS, 2015)

"La propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización" (Lemus, 2014)

Por lo tanto, acorde a lo indicado anteriormente se puede exponer que se refiere a confidencialidad al acceso de un recurso al cual solo se tenga la autorización definida por la organización.

Vulnerabilidad.

"……, referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones." (Alegsa, 2010)

De lo indicado anteriormente se puede exponer que una vulnerabilidad es una falencia de controles de seguridad necesarios los cuales pueden producir que un atacante comprometa ese sistema informático generando un incidente de seguridad el cual puede dar como resultado una pérdida de información.

Incidente de Seguridad.

"La violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita" (CERT, 2013)

"……..., indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información" (Normalización, 2010)

Por lo tanto se puede concluir que un incidente de seguridad es un evento de seguridad ocasionado por una violación a un sistema informático, el cual genera un riesgo que afecta a la seguridad de la información.

Riesgo.

"Contingencia o proximidad de un daño" (Diccionario de la Lengua Española, 2010).

"El potencial para un resultado adverso o no deseado como resultado de un incidente, evento u ocurrencia, según lo determine la probabilidad de que una

amenaza en particular explote una vulnerabilidad particular, con las consecuencias asociadas" (NICCS, 2015)

Por lo tanto se puede indicar que un riesgo es el cálculo o aproximación realizada para lograr evidenciar la proximidad o el alcance que puede tener un atacante al comprometer un recurso informático.

Plan de Tratamiento de Riesgos.

La norma internacional NTE ISO/IEC 31000:2009, indica cómo se debe de realizar un plan de tratamiento de riesgos de manera correcta, por lo cual se ha realizado el análisis de la misma y se expone un extracto de la misma a continuación.

Valoración del riesgo.

Como primer paso se va a realizar la valoración del riesgo el cual según la normativa NTE ISO/IEC 31000:2009 define como valoración de riesgo al "proceso total de identificación de riesgo, análisis del riesgo y evaluación del riesgo", acorde a lo indicado anteriormente se expone lo siguiente.

Identificación del Riesgo.

La organización debería de identificar el origen del riesgo, las áreas de impacto, los eventos y sus causas y consecuencias potenciales. El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podría crear, aumentar, prevenir, degradar o retrasar el logro de los objetivos. Es importante identificar los riesgos asociados a la no búsqueda de una oportunidad. La identificación exhaustiva es crítica porque un riesgo que no se identifique en esta fase no será incluido en el análisis posterior.

La identificación debería incluir los riesgos independientemente de si su origen está o no bajo control de la organización, aun cuando el origen del riesgo o su causa pueden o no ser evidentes. La identificación del riesgo debería incluir el examen de los efectos colaterales de las consecuencias particulares, incluyendo los efectos en cascada y acumulativos. También se debería considerar un rango amplio de consecuencias incluso si el origen del riesgo o su causa pueden o no ser evidentes. Al igual que la identificación de lo que podría suceder, es necesario considerar las causas y los escenarios posibles que muestran que las consecuencias se podrían presentar. Se recomienda considerar todas las causas y consecuencias significativas.

La organización debería aplicar herramientas y técnicas para la identificación del riesgo que sean adecuadas a sus objetivos y capacidades, y a los riesgos que se enfrenten. La información pertinente y actualizada es importante para identificar los riesgos. Esta información debería incluir, siempre que sea posible, la información básica. En la identificación del riesgo se debería de involucrar las personas con el conocimiento apropiado.

Análisis de Riesgo

El análisis de riesgo implica el desarrollo y la comprensión del riesgo. Este análisis brinda una entrada para la evaluación del riesgo y para las decisiones sobre si es necesario o no tratar los riesgos y sobre las estrategias y métodos más adecuados para su tratamiento. El análisis del riesgo también brinda una entrada para la toma de decisiones, en la cual se deben de hacer elecciones y las opciones implican diversos tipos de niveles de riesgo.

El análisis de riesgo involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, la probabilidad de que tales

consecuencias puedan ocurrir. Se deberían de identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo es analizado determinando las consecuencias y su probabilidad. Un evento puede tener consecuencias múltiples y pueden afectar a objetivos múltiples. También se deberían de considerar los controles existentes y eficiencia.

El análisis de riesgo se puede realizar con diversos grados de detalle, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles. El análisis puede ser cualitativo, cuantitativo o una combinación de ambos, dependiendo de las circunstancias.

El objetivos del análisis de riesgos es, "lograr establecer el riesgo total (o exposición bruta al riesgo) y luego el riesgo residual, tanto sea en términos cuantitativos o cualitativos" (Sena, 2004), de la misma forma expone también que "cuando se refiere al riesgo total, se trata de la combinación de los elementos que lo conforman. Comúnmente se calcula el valor del impacto promedio por la probabilidad de ocurrencia para cada amenaza y activo", por lo tanto, realizando el análisis de lo expuesto anteriormente por el autor se puede definir la siguiente fórmula para realizar el análisis de riesgo.

RT (Riesgo Total) = probabilidad x impacto promedio.

"A este cálculo se debe agregar el efecto de medidas mitigantes de las amenazas, generándose el riesgo residual. El riesgo residual es el riesgo remanente luego de la aplicación de medidas destinadas a mitigar los riesgos existentes."(Sena, 2004), por lo tanto se puede exponer que para un correcto análisis de riesgo es necesario identificar la probabilidad de ocurrencia y el impacto promedio que tendría ese recurso informático al ser comprometido, al resultado de este se tendría que

calcular el efecto de medidas o controles para mitigar las posibles amenazas dando como resultado un riesgo residual.

Evaluación del riesgo.

El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basada en los resultados de dicho análisis, a acerca de cuáles riesgos necesitan tratamiento y la prioridad vara la implementación del tratamiento.

La evaluación del riesgo implica la comparación del nivel de riesgo observado durante el proceso de análisis y de los criterios del riesgo establecidos al considerar el contexto. Con base en esta comparación, se puede considerar la necesidad de tratamiento.

En las decisiones se debería tener en cuenta el contexto más amplio del riesgo e incluir consideración de la tolerancia de los riesgos que acarrean otras partes diferentes de la organización que se benefician de los riesgos. Las decisiones se deberían tomar de acuerdo con los requisitos legales, reglamentarios y otros

Tratamiento del riesgo.

Acorde a la normativa NTE ISO/IEC 31000:2009 define como tratamiento de riesgo al proceso que “involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica”, por lo tanto según lo indicado anteriormente se expone lo siguiente.

El tratamiento de riesgos implica un proceso constante de:

- Valoración del tratamiento del riesgo.
- Decisión sobre si los niveles de riesgo residual son tolerables.

- Si no son tolerables, se genera un nuevo tratamiento para el riesgo.
- Valoración de la eficacia de dicho tratamiento.

Las elecciones para el tratamiento del riesgo no esencialmente son bilateralmente excluyentes ni apropiadas en todas las circunstancias. Las opciones pueden contener las siguientes:

- Evadir el riesgo al resolver no iniciar o continuar la actividad que lo originó.
- Aumentar el riesgo para conseguir una oportunidad.
- Descartar o retirar la fuente del riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con una o varias de las partes, incluyendo los contratos y la financiación del riesgo.
- Suspender el riesgo mediante una decisión informada.

MAGERIT.

Es una metodología que "implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información" (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

Existe una gran cantidad de aproximaciones cuando se analiza los posibles riesgos que pueden afectar directamente o indirectamente a los sistemas, por lo general el objetivo del análisis de riesgos a los sistemas es para tener conocimiento del nivel de seguridad que pueden tener los sistemas. Uno de los mayores retos de toda organización al conocer estas aproximaciones es la complejidad del problema al

que se enfrentan ya que existe muchos elementos que considerar y en caso de no tener un nivel considerado de rigurosidad las conclusiones tomadas pueden llegar a ser de poco fiar. Por lo tanto con la ayuda de Magerit se consigue aproximaciones metódicas las cuales no dan cavidad a una improvisación, ni dependen únicamente del análisis arbitrario.

De acuerdo al Ministerio de Hacienda y Administraciones Públicas de España (2012), en su ponente ilustración *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método,* indica que la metodología de MAGERIT busca los siguientes objetivos.

Objetivos Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Objetivos Indirectos:

1. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Esta metodología busca con sus objetivos establecer un procedimiento que abarca de manera completa un tratamiento de riesgos dentro de la organización tal como lo indica la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2001, la cual dice en el numeral **4.2.2a)** *Formular e Implementar un plan de tratamiento de riesgos que identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuados para gestionar los riesgos de la*

seguridad de la información (véase 5); y en el numeral **4.2.2b*)*** *Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que tengan en cuenta la financiación y la asignación de funciones y responsabilidades*, por lo cual esta metodología sería de gran apoyo para el diseño correcto de una matriz de tratamiento de riesgos como parte del Sistema de Gestión de Seguridad de la Información.

De manera adicional, se puede considerar una ventaja del uso de esta metodología que todas las decisiones que se tomen y deban de valorarse por la dirección tendrán un fundamento considerable y estas decisiones podrán ser defendidas fácilmente.

El Ministerio de Hacienda y Administraciones Públicas de España (2012), expone en la versión tres de la metodología de Magerit tres libros, los cuales se resumen a continuación.

El Método.

En el primer libro se indican las pautas y elementos estándares para la realización y planificación del análisis de gestión de riesgos, identificación y categorización de los activos, procedimientos para lograr un correcto análisis de riesgos, la consideración de las amenazas, la estimación de las vulnerabilidades y la estimación de impactos.

Catálogo de Elementos.

Esta guía facilita el trabajo de las personas involucradas en el proyecto ya que proporciona elementos estándar que pueden adscribirse rápidamente, enfocándose en

el objeto de análisis, por otra parte equipara los resultados de los análisis, promoviendo una terminología y criterios homogéneos los cuales van a permitir integrar los análisis realizados de diferentes equipos. De manera detallada se puede exponer que esta guía indica las pautas y elementos estándares en cuanto a tipos de activos, dimensiones de valoración de los activos, criterios de valoración, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

Guía Técnica.

Esta guía suministra una seria de técnicas las cuales se ejecutan para poder llevar a cabo proyectos de análisis y gestión de riesgos, entre las principales técnicas incluyen.

- Técnicas Específicas.
- Técnicas Algorítmicas.
- Arboles de Ataques.
- Análisis Costo Beneficio.
- Diagramas de Flujo.
- Diagramas de Procesos.
- Técnicas Gráficas.
- Planificación de Proyectos.
- Sesiones de Trabajo.
- Valoración Delphi.

Sistema de Gestión de la Seguridad de la Información.

"Un SGSI 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, implementación, 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" (Federico Pacheco, 2010).

EL SGSI es un documento que ayudará a establecer los procedimiento necesarios para una realizar una correcta gestión de la seguridad de la información, estos procedimientos deberían ir alineados al modelo de negocio de la organización para de esta manera llegar a una operación, mantenimiento y actualización eficiente del sistema, esto permitirá obtener un mayor nivel de integridad, disponibilidad y confidencialidad a los procesos más críticos de la organización.

El significado de información dentro del campo de la seguridad de la información se define como el conjunto de datos establecidos en dominio de una organización que ostenten valor para la misma, de forma independiente del medio como se la transmita o se la almacene (impresa en papel, digitalmente, email, etc.).

El Sistema de Gestión de Seguridad de la Información o SGSI se apoya en una norma o estándar internacional la ISO 27001, que permite identificar o evaluar los niveles de efectividad de los controles y procedimientos de seguridad que se encuentran implementados y operando en la organización, esto es en otras palabras evaluar los niveles para mantener o preservar la integridad, disponibilidad y confiabilidad de la información.

Fundamentos del SGSI.

"En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la

organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI". (Agustín López Neira, 2012)

Por lo tanto se puede indicar que para lograr que la información sea gestionada de manera eficiente se debe de identificar primeramente su período de vida y los aspectos de vital relevancia amparados para certificar su confiabilidad, disponibilidad e integridad.

Uso del SGSI.

"La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos". (Comunidad ISO27001.es, 2012)

Las entidades y sus sistemas informáticos hoy en día se encuentran expuestas a una innumerable cantidad de amenazas, un atacante puede llegar a aprovecha una vulnerabilidad que exista en un sistema, esto puede ocasionar que se llegue a comprometer a activos críticos de información en muchas formas tales como espionaje, fraudes, etc.

Otro de los aspectos fundamentales del SGSI es que brinda nuevas oportunidades de negocio, ya que logra establecer lazos de confianza con otras entidades o con clientes, que por lo general dentro de su política organizacional necesita mantener la confidencialidad e integridad de la información como requisito fundamental para establecer alianzas estratégicas por ejemplo: Instituciones Bancarias, Instituciones Militares, etc.

Beneficios del SGSI.

Llegar a la decisión de diseñar e implementar un Sistema de Gestión de Seguridad de la Información es un reto muy interesante, ya que por lo general genera cambios drásticos internamente, y esto genera costos considerables para la entidad en la que se está implementado, estos cambios siempre traen beneficios y estos beneficios son los que permiten marcar una diferencia considerable en el mercado, entre los beneficios que logrará obtener, se encuentran los siguiente:

- ***Cumplimiento de normativas vigentes***: un SGSI facilita de manera considerable el cumplimiento de diversos estándares o normativas de cumplimiento que estén relacionadas con la seguridad de la información.
- ***Reconocimiento corporativo***: El diseño e implementación exitosa de un SGSI permite a la entidad obtener la certificación reconocida internacionalmente *NTE INEN-ISO/IEC 27001:2011*, esto beneficia a la organización tener un prestigio en el mercado de la profesionalidad de la organización y es una garantía de su correcto funcionamiento.
- ***Certifica la continuidad del negocio:*** El desarrollo de un SGSI alinea los objetivos de la dirección y los procesos del negocio con la protección de sus activos de información, lo cual disminuye el riesgo ante amenazas que atenten con la seguridad de la información.

Declaración de Aplicabilidad.

"La Declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información." (Kosutic, 2011).

Mediante el tratamiento de riesgos se logró identificar los controles que debían implementarse, inicialmente se identificó los riesgos que fuese necesario disminuir. Sin embargo, en la Declaración de Aplicabilidad se debe de identificar los controles necesarios por diversas razones; por ejemplo, por temas legales, por requisitos contractuales, por otros procesos, etc.

Cuando se realiza el informe de la evaluación de riesgos por lo general suele resultar muy largo, ciertas organizaciones o entidades pueden llegar a identificar algunos miles de riesgos; por lo tanto, un informe con este tipo de características no suele resultar realmente útil en el uso operativo del día a día. Por el contrario, la Declaración de Aplicabilidad es realmente breve ya que tiene 133 filas (Cada una de estas representa un control); esto permite que pueda ser expuesta ante la alta dirección y que pueda ser actualizada.

En la Declaración de Aplicabilidad se debe de documentar si cada control aplicable ya se encuentra implementado. Una muy buena práctica la cual facilita la auditoría en el momento de la certificación es describir como se ha implementado cada control que se ha aplicado, detallando brevemente el procedimiento vigente o la solución de seguridad que se utiliza.

De lo analizado anteriormente se puede concluir que la Declaración de Aplicabilidad es el documento principal donde la organización define lo que controles de seguridad se implementan para conseguir asegurar la información.

Análisis de Brechas.

"…., es una herramienta de planificación estratégica que ayuda a comprender el estado actual, dónde se quiere llegar y cómo se va a llegar." (Rob Kelly, 2009).

Por medio del análisis de brechas se va a lograr identificar el estado real de una organización en un momento preciso, con respecto al cumplimiento de mecanismos de control y controles de seguridad ya implantados, tal como demanda la norma técnica NTE INEN-ISO/IEC 27001:2011.

FODA.

"…., la construcción de un balance estratégico, así los aspectos fuertes conforman los activos competitivos mientras que los aspectos débiles son los pasivos competitivos."(A. Strickland, 2006).

Al utilizar ésta herramienta, se va a lograr evidenciar las fortalezas, oportunidades, debilidades y amenazas que comprende el análisis y diseño de un Sistema de Gestión de Seguridad de la Información, aplicado a un modelo de negocio dedicado a la comercialización y distribución de productos químicos.

PESTEL.

"…., el esfuerzo realizado para captar con precisión las implicaciones para una empresa que se derivan del ambiente político, económico, social, tecnológico, legislativo y ecológico en el que debe desenvolverse" (Antonio Pulido, 2006).

Acorde a lo expuesto anteriormente, se puede indicar que por medio de ésta herramienta, se va a proporcionar el impacto que tendría realizar el análisis y diseño de un Sistema de Gestión de Seguridad de la Información, en organizaciones que se dediquen a la comercialización y distribución de productos químicos, en el ámbito político, económico, social, tecnológico, legislativo y ecológico.

PHVA (Planificar – Hacer – Verificar - Actuar).

"……, es un modelo muy bien conocido para mejoramiento continuo de procesos (continuous process improvement "CPI")." (Nancy Tague, 2006)

"Enseña a organizaciones a planear una acción, hacerla, revisarla para ver cómo se conforma al plan y actuar en lo que se ha aprendido." (ASQ y la Holmes Corp., 2005)

Dado que éste proyecto de investigación se encuentra aplicado a los procesos de comercialización y distribución de productos químicos, se puede considerar que éste modelo sería el más adecuado para gestionar y mantener el Sistema de Gestión de Seguridad de la Información, ya que cumple con un ciclo (planificar, hacer, verificar y actual) y busca el mejoramiento continuo de procesos.

Herramienta para automatizar el proceso del SGSI (e-PULPO).

¿Qué es e-PULPO?

Es una integración de herramientas de software libre y desarrollos de ingenierías para dar cobertura a la gestión de manera automatizada y efectiva de:

- LOPD.
- ENS.
- SGSI (ISO 27001)
- ITIL (ISO 20000)
- PCI DSS.

Funcionalidades de e-PULPO

Dentro de las funcionalidades más relevantes que posee e-PULPO se tienen las siguientes.

- Inventario automático.
- Gestión de inventario, tickets y diagramas de red.
- Valoración de activos y dependencias.
- Análisis de gestión de riesgos.
- Análisis de impacto y continuidad de operaciones.
- Gestión de planes de acción.
- Gestión documental.
- Gestión de incidentes.
- Gestión LODP.
- Foros colaborativos.
- Bases de Conocimiento.
- Cuadro de mandos (desarrollo propio).
- Formación y difusión.

Requerimientos mínimos para la instalación de la herramienta e-PULPO.

De acuerdo a lo indicado en el sitio oficial del software e-PULPO (***e-pulpo****.com*), se indican los requerimientos mínimos de hardware para lograr una exitosa instalación de la herramienta e-PULPO, por lo tanto se puede indicar que lo siguiente.

Dentro de los requerimientos mínimos recomendados se tiene.

- Doble procesador con cuatro núcleos cada uno.
- 8Gb de memoria RAM.
- Espacio en disco como mínimo de 500 Gb.

Como información adicional, esta solución es compatible para ambientes de virtualización con VMWare Sphere 5.0 o superior.

Cumplimiento de e-PULPO para un SGSI.

La norma NTE INEN-ISO/IEC 27001:2001 es un estándar asociado a la seguridad de la información la cual pertenece a la serie de los 27000, por lo tanto la herramienta e-PULPO no solo se enfoca en las especificaciones del SGSI como indica la norma NTE INEN-ISO/IEC 27001:2001, sino que abarca de una manera más complementaria las siguientes normas.

- ISO 27000 = Fundamentos
- ISO 27001 = Especificaciones de un SGSI (Certificable)
- ISO 27002 = Código de buenas prácticas
- ISO 27003 = Guía de implantación
- ISO 27004 = Métricas e Indicadores
- ISO 27005 = Guía para el Análisis y Gestión del Riesgo
- ISO 27006 = Especificaciones para organismos certificadores
- ISO 27007 = Guía de requisitos para entidades auditoría y certificación.

De manera adicional se expone a continuación en la siguiente tabla, de manera detallada el soporte que tiene e-PULPO como herramienta para la automatización del ciclo de implementación, operación, supervisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información.

Tabla 1: Cumplimiento de e-PULPO para el diseño del SGSI.

Apartado.	**Soporte en e-PULPO**
4.2.1. Creación del SGSI	Completando previamente el control 7.1.1 (ISO 27002)

a) Gestionar y Elaborar el alcance.	e-PULPO dispone de un módulo de Gestión Documental para gestionar la documentación del alcance del SGSI
b) Definir una política.	e-PULPO dispone de un módulo de Gestión Documental para gestionar la documentación del alcance del SGSI
c) Especificar la metodología de evaluación de riesgos.	e-PULPO dispone de un módulo de Gestión Documental para gestionar la documentación del alcance del SGSI
d) e) f) Análisis y gestión de riesgos.	E-PULPO está integrado con PILAR (herramienta para el análisis de riesgos), permite crear vía web activos genéricos en para la valoración de los procesos de negocio, ubica los activos en capas, grupos y dominios de seguridad, permite la asignación de clases a los activos, permite establecer las dependencias entre activos, seleccionar los objetivos de control y valorar las salvaguardas.
h) i) Aprobar el informe de análisis de riesgos de PILAR.	e-PULPO dispone de un módulo de Gestión Documental para gestionar el almacenamiento y aprobación del análisis y gestión de riesgos generado con PILAR
j) Declaración de aplicabilidad.	e-PULPO está integrada con PILAR (herramienta para el análisis de riesgos), a través de la que se elabora el SOA, que luego se almacena en el

	módulo de gestión documental.
4.2.2 Implementación y operación del SGS	
a) Plan de Tratamiento de riesgos.	e-PULPO lo tiene cubierto, como se ha indicado para el punto 4.2.1.d) de la norma.
b) c) Planificar y gestionar el plan de tratamiento de riesgos.	e-PULPO permite hacer el seguimiento de las acciones a realizar a través del módulo de "Gestión de Planes de Acción"
d) Definición de métricas para evaluar la eficacia de los controles.	e-PULPO dispone de un módulo de "Métricas y Cuadros de Mando" que permite la creación de métricas y hacer su seguimiento con alertas
e) Implementar programas de formación y concientización.	e-PULPO permite implementar estos programas desde su módulo de "Formación y Concienciación", a través de una plataforma de tele formación.
f) Gestionar la operación del SGSI.	La gestión de la operación la realiza el propio SGSI
g) Gestionar los recursos del SGSI	e-PULPO ayuda a la gestión diaria de los recursos para la seguridad a través de la planificación establecida en el módulo de "Gestión de Planes de Acción" (donde se pueden observar las tareas asignadas a cada recurso y su disponibilidad con diagramas de Gantt) y Gestión de Tickets (donde se pueden observar las

	solicitudes e incidencias que debe resolver cada recurso, y en qué momento está planificado ejecutarlo directamente en el calendario)
h) Detección temprana de eventos de seguridad.	e-PULPO realiza un seguimiento de las últimas vulnerabilidades publicadas del software instalado. Además, gracias a la conexión con AlienVault OSSIM (herramienta SIEM basada en software libre), monitorizamos los sistemas, recibimos alertas y actualizamos en tiempo real el análisis de riesgos
4.2.3 Supervisión y revisión del SGSI	
a) Procedimientos de supervisión y revisión	
1) Detectar Errores.	e-PULPO, gracias a la conexión con AlienVault OSSIM (herramienta SIEM basada en software libre), monitoriza los sistemas y recibe alertas en caso de caída.
2) Identificar Debilidades.	e-PULPO, gracias a la conexión con AlienVault OSSIM (herramienta SIEM basada en software libre), realiza auditorías (hacking ético) y recibe alertas en caso de detectar vulnerabilidades.
b) Gestión de Informes de Auditorias SGSI.	e-PULPO ofrece la gestión de los informes de auditoría desde su módulo “Gestión Documental”.

c) Gestión de actas de reunión, revisión por la dirección, etc.	e-PULPO permite desde el módulo "Gestión Documental" la gestión de las actas de reunión y gestión de contenidos para que puedan ser revisadas por la dirección.
4.2.4 Mantenimiento y mejora del SGSI.	No aplica a la funcionalidad de e-PULPO como plataforma
4.3 Requisitos de la documentación	e-PULPO permite gestionar la documentación además de proporcionar a través de workflows ciclos para la vida de cada documento.
5 Responsabilidad de la Dirección	
5.2 Gestión de los recursos	e-PULPO permite la gestión de los recursos desde los módulos "Gestión de Activos y Tickets" y "Gestión de Planes de Acción".
5.2.1 Provisión de los recursos	e-PULPO permite gestionar la provisión de recursos organizando, identificando y supervisando las acciones desde el módulo "Gestión de Planes de Acción".
5.2.2 Concienciación, formación y capacitación	e-PULPO dispone del módulo de "Formación y concienciación" que permite llevar a cabo acciones formativas para asegurar que el personal dispone del conocimiento adecuado para llevar a cabo sus tareas asignadas.
5. Auditorías internas del SGSI	
a) Cumplen los requisitos de	e-PULPO, a través de su conexión con PILAR,

esta norma, legislación y normativas.	permite medir los niveles de cumplimiento
b) Cumplen los requisitos de seguridad de la información identificados	e-PULPO permite verificar el cumplimiento de los requisitos que se definan en su módulo "Gestión de Cuadros de Mando".
c) Se implantan y se mantienen de forma efectiva	e-PULPO permite verificar el nivel de implantación definidos con métricas en su módulo "Gestión de Cuadros de Mando".
d) Dan el resultado esperado	e-PULPO permite verificar a través del módulo" Cuadros de Mando" si se cumplen las expectativas en los resultados.
6. Revisión del SGSI por la Dirección	
7.1 Generalidades	e-PULPO permite que la Dirección revise la conveniencia y eficacia del SGSI desde los "Cuadros de Mando" definidos.
7.2 Datos iniciales de la revisión	Desde las diferentes funcionalidades de e-PULPO, como el módulo de "Gestión Documental", se pueden gestionar los datos para las auditorias, comentarios, procedimientos, técnicas, estado de las acciones preventivas, y recomendaciones de mejora
7.3 Resultados de la revisión	e-PULPO permite almacenar los informes resultantes en su "Gestor documental".
8 Mejora del SGS	

a) Plan de acciones correctivas a una no conformidad	e-PULPO facilita la creación de tickets sobre acciones desde su módulo de “Gestión de Activos y Tickets”, o desde el módulo de “Gestión de planes de acción”.
b) Plan de acciones preventivas a una no conformidad	e-PULPO facilita la creación de tickets sobre acciones desde su módulo de “Gestión de Activos y Tickets”
c) Gestionar los planes de acciones correctivas y preventivas	e-PULPO permite el seguimiento así como la notificación automática para el seguimiento de las acciones desde su módulo de “Gestión de Activos y Tickets”.

Fuente: (Ingeniería e Integración Avanzadas (Ingenia), 2008).

Capturas del software e-PULPO.

A continuación se exponen las siguientes capturas (Figura 2, 3, 4 y 5) las cuales muestran la estructura de la interfaz del software e-PULPO y lo amigable que éste puede llegar a ser**.**

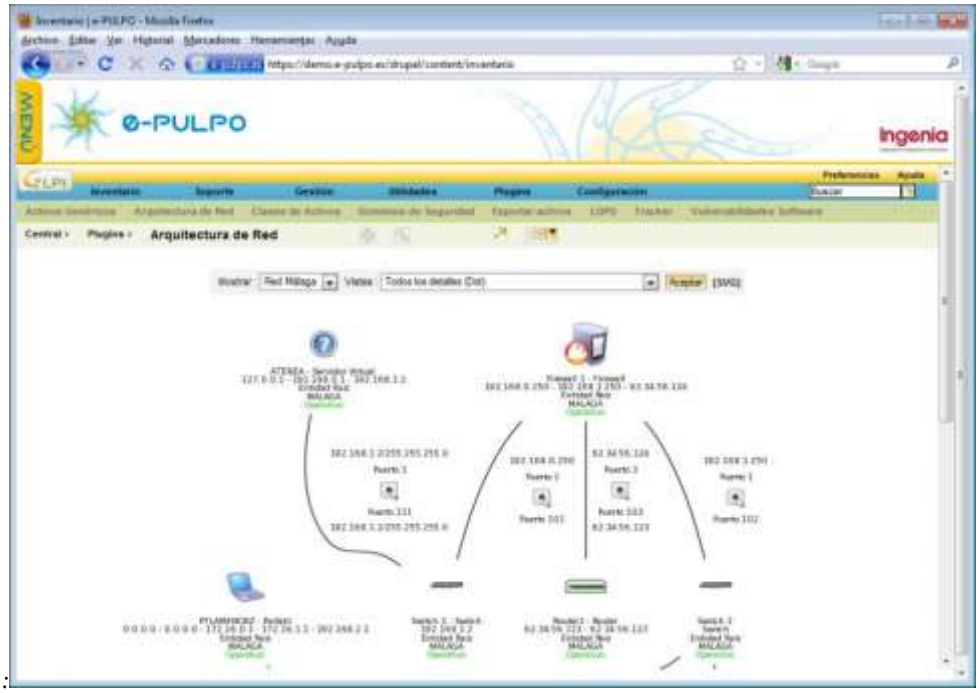


Figura 2: Interfaz del diagrama de red de e-PULPO.

Fuente: (Ingeniería e Integración Avanzadas (Ingenia), 2008).

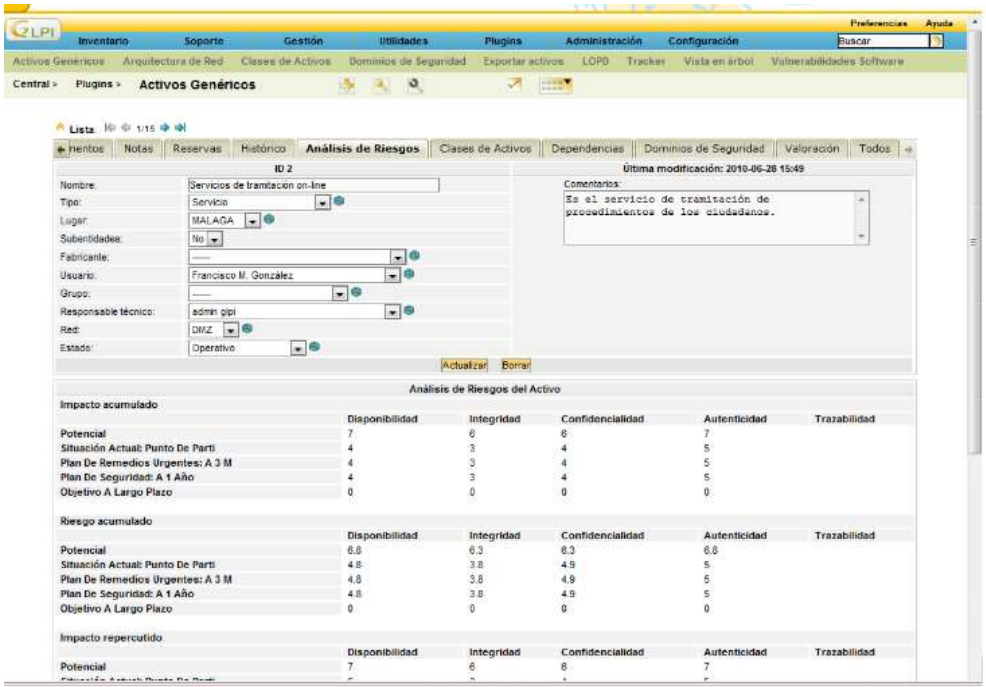


Figura 3: Interfaz de inventarios de activos de e-Pulpo.

Fuente: (Ingeniería e Integración Avanzadas (Ingenia), 2008).

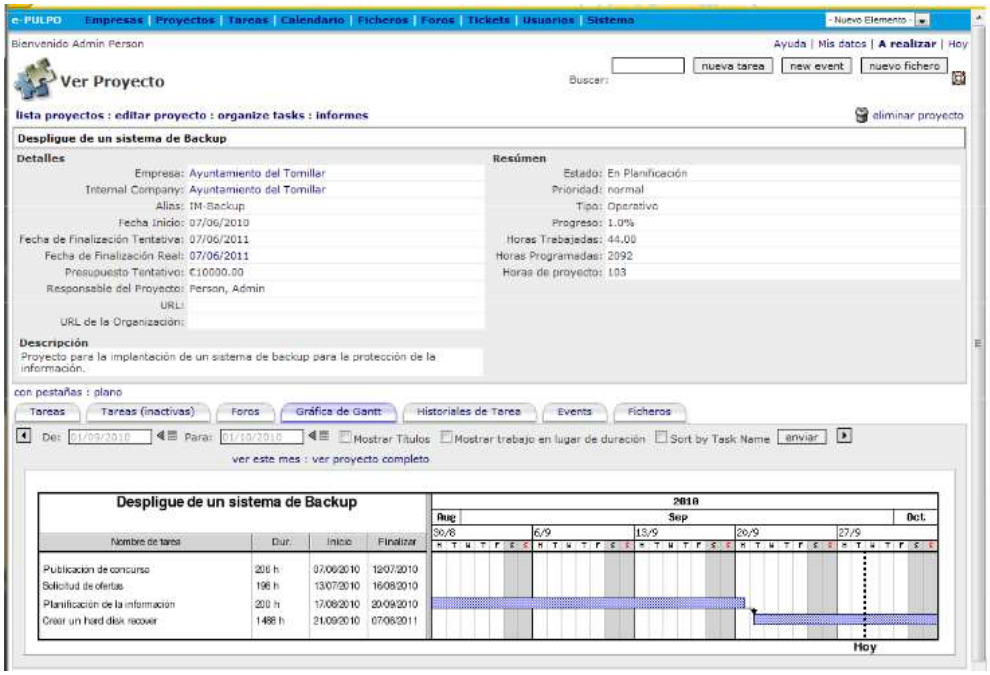


Figura 4: Interfaz de inventarios de tareas o procesos de e-Pulpo.

Fuente: (Ingeniería e Integración Avanzadas (Ingenia), 2008).

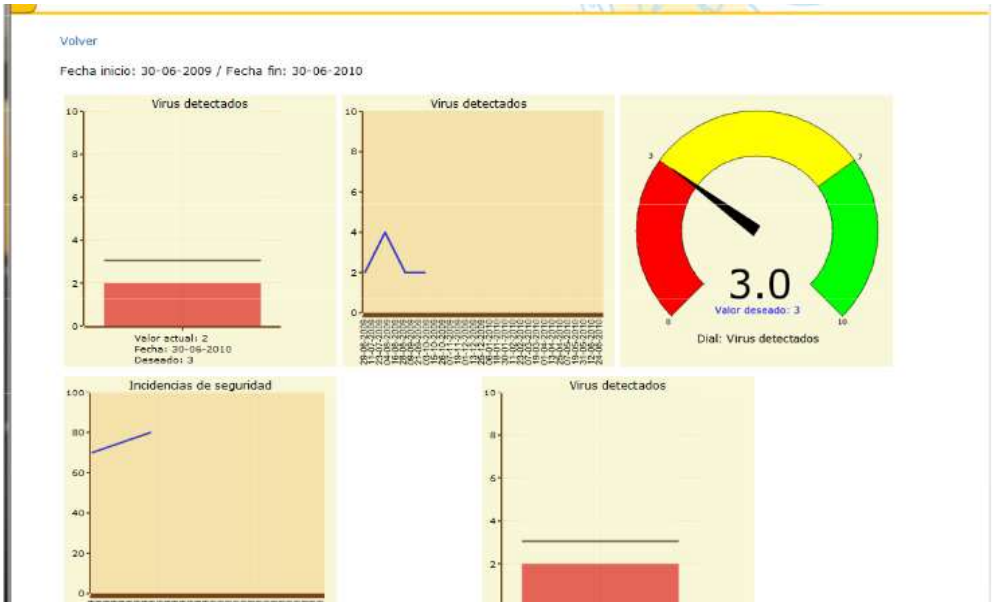


Figura 5: Muestras de amenazas y riesgos encontrados.

Fuente: (Ingeniería e Integración Avanzadas (Ingenia), 2008).

2.3. Marco Normativo.

La serie 27000.

"La serie ISO 27000 es la que aglomera todas las normativas en materia de seguridad de la información. Las más importantes de esta familia son las normas ISO 27001 e ISO 27002" (Bortnik , 2010).

A continuación se ha desarrollado una breve relación de cada una de las normas de la familia 27000 (tabla 2), esta información fue obtenida por un organismo de normalización encargada de la publicación de norma AENOR.

Tabla 2: Relación de las normas de la serie ISO 27000

Normas.	**Temática**
ISO 27000.	Gestión de la Seguridad de la Información.
ISO 27001.	Especificaciones para un SGSI (Certificable).
ISO 27002.	Códigos de Buenas Prácticas.
ISO 27003.	Guía de Implantación de un SGSI.
ISO 27004.	Sistema de Métricas e Indicadores.
ISO 27005.	Guía de Análisis y Gestión de Riesgos.
ISO 27006.	Especificaciones para Organismos Certificadores del SGSI.
ISO 27007.	Guía para auditar el SGSI.
ISO/IEC TR 27008.	Guía de Auditoría de los controles seleccionados en el marco de implantación de un SGSI.
ISO/IEC 27010.	Guía para la gestión de la seguridad de la información cuando se comparte entre sectores u organizaciones.

Fuente: (Universidad Nacional Abierta y a Distancia – UNAD, 2013).

Evolución de las normativas de la seguridad de la información.

"A inicios de la década de los 90, el Departamento de Comercio e Industria del Reino Unido inició el desarrollo de una norma británica (en adelante BS), para proteger y regular la gestión de la seguridad en la empresa, y como respuesta a las peticiones de la industria, el gobierno y los comerciantes para crear una estructura común de seguridad de la información" (Robles & Rodriguez De Roa, 2006).

De cierta manera a este primer gran hito en la estandarización y normalización de la gestión de la seguridad de la información anteriormente mencionado le han seguido las siguientes.

Tabla 3: Evolución de las normativas de la seguridad de la información.

Año.	Norma.
1995	La primera norma aprobada oficialmente fue la (BS 7799:95) y nace como un código de buenas prácticas para la gestión de seguridad de la información.
1998	Se publica la norma BS 7799-2, en la que se recogen especificaciones para la gestión de la seguridad de la información y se exponen requerimientos certificables por primera vez.
1999	Se expone la segunda edición, en la que se añade "e-commence" al alcance de la norma. En aquella época, la Organización Internacional de Normalización (ISO) comienza a interesarse ya por los trabajos publicados por el Instituto inglés.
2000	ISO aprueba la norma ISO 17799 Parte 1, que es el Código de Práctica para los requisitos de gestión de seguridad de la información (no certificable). Esta norma está formada por un

	conjunto completo de controles que conforman las buenas prácticas de seguridad de la información, y que pueden ser aplicadas por toda organización con independencia de su tamaño.
2002	Se realiza la segunda revisión y se hace certificable la norma BS (BS 7799-2:2002), con el fin de armonizarla con otras normas de gestión tales como la ISO 9001:2000 y la ISO 14001:1996, así como con los principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).
2002	Se publica la norma UNE-EN ISO/IEC 17799/ 1:2002, en España.
2005	Se publica la norma ISO 27001, norma certificable y que reemplazará a la actual BS 7799-2.

Fuente: (Robles & Rodriguez De Roa, 2006).

¿Qué es la norma NTE INEN-ISO/IEC 27001:2011?

Según la norma técnica **NTE INEN-ISO/IEC 27001:2011** indica que "Esta norma proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debería ser fruto de una decisión estratégica de una organización". (Instituto Ecuatoriano de Normalización, 2010)

Por lo tanto por medio de este documento como modelo y siguiendo los procedimientos indicados en esta norma, se va a lograr obtener los procedimientos necesarios para realizar un diseño firme de un Sistema el cual va a proporcionar las políticas y procedimientos necesarios para la correcta gestión de la seguridad de información.

Acorde a la siguiente información indicada en la noma técnica **NTE INEN-ISO/IEC 27001:2011** indica que "Esta norma sirve para que cualquier parte interesada, ya sea interna o externa a la organización, pueda efectuar una evaluación de la conformidad". (Instituto Ecuatoriano de Normalización, 2010)

Por lo tanto si existe el diseño y la implementación correcta de este sistema es factible que se pueda medir la efectividad de la gestión de la seguridad de información y de la misma manera los niveles de integridad, disponibilidad y confiabilidad de los activos informáticos dentro de la organización, ya sean para fines de cumplimiento de estándares internaciones o para fines de cumplimento gubernamental.

Componentes de la norma NTE INEN-ISO/IEC 27001:2011.

Acorde a lo indicado en la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011, se exponen los siguientes componentes principales.

Tabla 4: Requisitos de norma técnica ecuatoriana INEN-ISO/IEC 27001:2011

Requerimiento / Elementos
4.1 Requisitos Generales La organización debe crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI documentando dentro del contexto de las actividades empresariales generales de la organización y de los riesgos que esta afronta. A efectos de esta norma, el proceso utilizado se basa en el modelo PCDA.
4.2.1 Creación del SGSI.
4.2.1a) Definir el alcance y los límites del SGSI en términos de las características de la actividad empresarial, de la organización, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier excusa del alcance.
4.2.1b) Definir una política del SGSI acorde con las características de la actividad empresarial, la organización, su ubicación, sus activos y tecnología.
4.2.1c) Definir el enfoque de la evaluación de riesgos de la organización.
4.2.1d) Identificar los riesgos.
4.2.1e) Analizar y valorar los riesgos
4.2.1f) Identificar y evaluar las opciones para el tratamiento de riesgos

Requerimiento / Elementos
4.2.1g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
4.2.1h) Obtener la aprobación, por parte de la Dirección, de los riesgos residuales propuestos.
4.2.1i) Obtener la autorización de la Dirección para implementar y operar el SGSI.
4.2.1j) Elaborar una declaración de aplicabilidad. Una declaración de aplicabilidad debe incluir lo siguiente: 1. Los objetivos de control y los controles seleccionados en 4.2.1g) y las justificaciones de su selección; 2. Los objetivos de control y los controles actualmente implementados (4.2.1e). 3. La exclusión de cualquier objetivo de control y control del anexo A y la justificación de esta exclusión.
4.2 Implementación y Operación del SGSI
4.2.2a) Formular un plan de tratamiento de riesgos que identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuados para gestionar los riesgos de la seguridad de la información (véase 5).
4.2.2b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que tengan en cuenta la financiación y la asignación de funciones y responsabilidades.
4.2.2c) Implementar los controles seleccionados en **4.2.1g,** para cumplir los objetivos de control.

Requerimiento / Elementos
4.2.2d) Definir el modo de medir la eficacia de los controles o de los grupos de controles seleccionados y especificar como tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir unos resultados comparables y reproducibles (Véase 4.2.3c)
4.2.2e) Implementar programas de formación y concienciación (Véase 5.2.2).
4.2.2f) Gestionar la Operación del SGSI.
4.2.2g) Gestionar los recursos del SGSI.
4.2.2h) Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad (Véase 4.2.3a)
4.2.3 Supervisión y Revisión del SGSI
4.2.3a) Ejecutar procedimientos de supervisión y revisión, así como otros mecanismos del control para:
4.2.3b) Realizar revisiones periódicas de la eficacia del SGSI teniendo en cuenta los resultados de las auditorias de seguridad, los incidentes, los resultados de las mediciones de la eficacia, las sugerencias así como los comentarios de todas las partes interesadas. Estas revisiones incluyen el cumplimiento de la política, y de los objetivos del SGSI, y la revisión de los controles de seguridad.
4.2.3c) Medir la eficacia de los controles para verificar si se han cumplido los requisitos de seguridad.

Requerimiento / Elementos
4.2.3d) Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles de riesgo aceptables que han sido identificados, teniendo en cuenta los cambios.
4.2.3e) Realizar las auditorías internas del SGSI en intervalos planificados. **Nota:** Las auditorías internas, a veces se denominan auditorias por primera parte, las lleva a cabo la propia organización.
4.2.3f) Realizar por parte de la Dirección una revisión del SGSI, con carácter regular para asegurar que el ámbito de aplicación sigue siendo adecuado y que se identifican mejoras del proceso del SGSI (Véase 7.1)
4.2.3g) Actualizar los planes de seguridad teniendo en cuenta las conclusiones de las actividades de supervisión y revisión.
4.2.3h) Registrar las acciones e incidencias que pudieran afectar a la eficacia o al funcionamiento del SGSI (Véase 4.3.3)
4.2.4 Mantenimiento y mejora del SGSI
4.2.4a) Implementar en el SGSI las mejoras identificadas
4.2.4b) Aplicar las medidas correctivas y preventivas adecuadas de acuerdo con los apartados 8.2 y 8.3, sobre la base de la experiencia en materia de seguridad de la propia organización y de otras organizaciones.
4.2.4c) Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle acorde con las circunstancias.
4.2.4d) Asegurar que las mejoras alcances los objetos previstos.
4.3 Requisitos de la Documentación
4.3.1a) Declaración documentada de la política.

Requerimiento / Elementos
4.3.1b) El alcance del SGSI
4.3.1c) Los procedimientos y mecanismos de control que soportan al SGSI.
4.3.1d) Una descripción de la metodología de evaluación de riesgo.
4.3.1e) El informe de evaluación de riesgos
4.3.1f) El plan de tratamiento de riesgos.
4.3.1g) Los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles
4.3.1h) Los registros requeridos por esta norma (4.3.3)
4.3.1i) La declaración de aplicabilidad
4.3.2 Control de Documentos
4.3.2a) Aprobar el formato de los documentos previamente a su distribución.
4.3.2b) Revisar, actualizar y volver a aprobar los documentos, según vaya siendo necesario.
4.3.2c) Asegurar que están identificados los cambios, así como el estado del documento que contiene la última revisión.
4.3.2d) Asegurar que las versiones correspondientes de los documentos estén disponibles.
4.3.2e) Asegurar que los documentos aparezcan legibles y fácilmente identificables.

Requerimiento / Elementos
4.3.2f) Asegurar que los documentos estén disponibles para todo el que lo necesita, y se transfieren, almacenan y destruyen de acuerdo con los procedimientos aplicables a su clasificación.
4.3.2g) Asegurar que los documentos procedentes del exterior estén identificados
4.3.2h) Asegurar que la distribución de los documentos sea controlada
4.3.2I) Prevenir el uso no intencionado de documentos obsoletos
4.3.2j) Aplicar una identificación adecuada a los documentos obsoletos que son retenidos con algún propósito.
4.3.3 Control de Registros
4.3.3 Se debe de crear y mantener registros para proporcionar evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
5. Responsabilidades de la dirección.
5.1 Compromiso de la Dirección. La dirección debe suministrar evidencias de su compromiso para crear, implementar, operar, superar, revisar, mantener y mejorar el SGSI.
5.2 Gestión de los Recursos.
5.2.1 Provisión de los Recursos. La organización debe determinar y proporcionar los recursos necesarios.
5.2.2 Concienciación, formación y capacitación. La organización debe de asegurarse de que todo el personal al que se hayan asignado responsabilidades definidas en el SGSI sea competente para llevar a cabo las tareas requeridas.

Requerimiento / Elementos
6. Auditorías Internas del SGSI Determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI. a) Cumplen los requisitos de esta norma, así como la legislación y normativas aplicables b) Cumplen los requisitos de seguridad de la información identificados. c) Se implantan y mantienen de forma efectiva. d) Dan el resultado esperado
7. Revisión del SGSI por la Dirección. Revisión por la dirección por lo menos una vez al año, para asegurar que se mantiene su conveniencia, adecuación y eficacia.
8. Mejora del SGSI.
8.1 Mejora Continua. La organización debe mejorar de manera continua la eficacia del SGSI, mediante el uso de la política y de los objetos de seguridad de la información, de los resultados de las auditorias, del análisis de la monitorización de eventos, de las acciones correctivas y preventivas y de las revisiones de dirección (Véase 7).

Requerimiento / Elementos
8.2 Acciones Correctivas El procedimiento documentado para las acciones correctivas debe definir los requisitos para: a) Identificar las no conformidades b) Determinar las causas de las no conformidades c) Evaluar la necesidad de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse. d) Determinar implantar las acciones de las correctivas necesarias e) Registrar los resultados de las acciones realizadas f) Revisar las acciones correctivas realizadas
8.3 Acciones Preventivas Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas potenciales. a) Identificar las posibles no conformidades y sus causas. b) Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades. c) Determinar e implementar las acciones preventivas necesarias. d) Registrar los resultados de las acciones adoptadas e) Revisar las acciones preventivas adoptadas.

Fuente: (Instituto Ecuatoriano de Normalización, 2010)

Elaborado por: Autor.

2.4. Formulación de Hipótesis.

2.4.1. Hipótesis General.

Al diseñar un Sistema de Gestión de la Seguridad de la Información basado en el apartado 4.3.1 del criterio de la norma *NTE INEN-ISO/IEC 27001:2011*, se logrará garantizar los niveles apropiados de integridad, disponibilidad y confidencialidad en un modelo de negocio dedicado a la comercialización y distribución de productos Químicos.

2.4.2. Hipótesis Específicas.

i. Al plantear el alcance del SGSI, se podrá indicar los controles y mecanismos de seguridad, que serán aplicados sobre los procesos de comercialización y distribución de productos químicos, para la protección de la información.

ii. Al formular la declaración documentada de la política, se podrá establecer los mecanismos de seguridad más idóneos para ejecutar procedimientos dentro de la organización de manera óptima y segura.

iii. Al establecer un plan de tratamiento de riesgos, se logrará identificar los posibles riesgos y vulnerabilidades que puedan afectar de manera directa o indirecta la integridad, confidencialidad e integridad de la información y de esta manera se podrá establecer los mecanismos más idóneos para mitigarlos.

iv. Al elaborar la declaración de aplicabilidad, se podrá establecer que controles de seguridad deben de ser implantados para garantizar la seguridad de la información.

2.5. Señalamiento de Variables.

A continuación se ha desarrollado el siguiente señalamiento de variables.

2.5.1 Variables Dependientes.

Para este proyecto de investigación se expone la siguiente variable dependiente.

- Diseño del Manual de Gestión de Seguridad de la Seguridad de la Información basado en el criterio de la norma técnica NTE-ISO/IEC 27001:2011.

2.5.2 Variables Independientes.

Para este proyecto de investigación se exponen las siguientes variables independientes.

- Políticas de Seguridad.
- Procedimientos y mecanismos de control.
- Metodología de Análisis de Riesgos.
- La Declaración de Aplicabilidad.

CAPÍTULO III
MARCO METODOLÓGICO

3.1. Modalidad de la Investigación.

En el desarrollo de este proyecto han utilizado varios tipos de estudios o investigación, entre estos:

a) Investigación de campo / teórica

La investigación de campo "… consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta" (Palella & Martins, 2010), por lo tanto acorde a lo mencionado se expone lo siguiente.

Esta investigación contempla un estudio teórico, en el que se analizan las propuestas más relevantes de reconocidos autores y expertos en el tema, en base a las que el autor desarrolla las ponencias científicas presentadas en el presente documento; adicionalmente es necesario llevar a cabo estudios de campo, puesto que es necesario para recabar información veraz, actualizada y directamente de la fuente.

b) Investigación Exploratoria

La investigación exploratoria es "… aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir, un nivel superficial de conocimientos" (Arias, 2012), por lo tanto acorde al análisis realizado se expone lo siguiente.

Esta investigación es de nivel exploratorio debido a que el desarrollo de este proyecto es aplicado sobre un modelo de negocio que ha sido poco estudiado, por

cual se espera que sus resultados favorables sirvan como guía para el resto de organizaciones que tengan un modelo de negocio similar.

c) Investigación descriptiva.

La investigación descriptiva "…., consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere" (Arias, 2012), por lo tanto acorde a lo indicado se ha podido llegar a la siguiente conclusión.

Este proyecto es de carácter descriptivo puesto que se describe un Sistema de Gestión de Seguridad de la Información, permitiendo de esta manera comprobar sistemáticamente y progresivamente las necesidades del modelo de negocio.

3.2. Métodos de Investigación.

Durante el desarrollo de este proyecto se tesis se utilizarán los siguientes métodos de investigación.

a) Método Inductivo-Deductivo.

Se manejará el método inductivo deductivo, ya que ayudará a la identificación y determinación de los controles de seguridad o aspectos que en base al criterio de la normativa son aplicables al modelo de negocio, así como descartar aquellos que no sean necesarios.

b) Método Analítico-Sintético.

Fragmentación y distinción de los componentes del Sistema de Gestión de Seguridad de la Información. Este método de análisis y síntesis se utilizará para la obtención de un cuerpo compuesto el cual es el Sistema de Gestión de Seguridad de

la información a partir de compuestos más sencillos los cuales son todos los controles y apartados que van a ser aplicados para el modelo de negocio.

3.3. Instrumentos de recolección de datos.

Para el desarrollo de este proyecto de tesis se han utilizado los siguientes mecanismos de recolección de información:

a) Cuestionario.

Por medio de un análisis realizado a las preguntas formuladas a principales organizaciones con un modelo de negocio de comercialización y distribución de productos químicos del mercado ecuatoriano se podrá evidenciar si este proyecto cumple con los objetivos y expectativas previamente establecidas.

b) Observación.

Por medio de la observación se logrará obtener la mayor cantidad de datos que aporte de manera relevante a este proyecto de investigación, con esto se logrará registrarla para realizar un análisis posterior.

3.4. Población y muestra

3.4.1 Población.

La población considerada en este proyecto de investigación representa a las empresas dedicadas a la comercialización y distribución de productos químicos en el Ecuador, se enfoca específicamente a los Administradores de infraestructura y Oficiales de Seguridad de la Información, debido a que estas personas son responsables de los departamentos de tecnología y seguridades de las organizaciones.

3.4.2 Muestra.

Las principales empresas dedicadas a la comercialización y distribución del sector químico en Ecuador son Ecuaquímica, Brenntag, Quimpac y Quimasa, tomando como fuente confiable la publicación realizada por la revista Vistazo en la cual según un análisis realizado de ingresos anuales, expone las principales empresas que se especializan en este sector dentro de un ranking de 500 mayores empresas de diversos sectores en el Ecuador.

Figura 6: Principales Industrias Químicas del Ecuador.

Fuente: (Superintendencia de Compañías, Servicio de Rentas Internas (SRI), Instituto Ecuatoriano de Seguridad Social (IESS) e información directa proporcionada por las empresas, 2014).

3.4. Operacionalización de las Variables.

A continuación se expone la declaración y operacionalización de las variables.

Tabla 5: Declaración y Operacionalización de las variables.

VARIABLES	TIPOS	CONCEPTOS	INDICADORES
Diseño un Sistema de Gestión de Seguridad de la Seguridad de la Información basado en el criterio de la norma técnica NTE-ISO/IEC 27001:2011.	Dependiente	Documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI	Ayudar a gestionar la información y los recursos informáticos de manera óptima y segura, va a brindar un reconocimiento corporativo y va a brindar nuevas oportunidades de negocio.
Políticas de Seguridad.	Independiente	Garantiza que la dirección proporcione indicaciones y dará apoyo a la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y normas aplicables.	Desarrollo de políticas de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información.

Procedimientos y mecanismos de control.	Independiente	Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.	Documentación de procedimientos y diseño de controles.
Metodología de Análisis de Riesgos.	Independiente	Describe las fases o etapas a aplicar, para elaborar el análisis de riesgo informático.	Documentación de una metodología para la identificación y tratamiento de riesgos.
La Declaración de Aplicabilidad.	Independiente	Documento que contiene los objetivos de control y controles del Anexo A, con sus debidas exclusiones, este documento permite conocer, el estado actual de los controles de seguridad dentro de la organización.	Desarrollo del documento Declaración de Aplicabilidad.

Fuente: (Instituto Ecuatoriano de Normalización, 2010)

Elaborado por: Autor.

3.5. Plan de recolección y procesamiento de la información.

El plan de recolección y procesamiento de la información ayudará a identificar las actividades que se realizarán en este proyecto de investigación, por esta razón se describen cada una de sus partes.

A. Aprobación del anteproyecto.

En la aprobación del anteproyecto de tesis se expuso el tema de estudio que se va a realizar para el desarrollo del documento de tesis. En el mismo documento se realizó la justificación, la definición de objetivos y variables y se especificó el tiempo de ejecución de la propuesta.

B. Inicio del proyecto.

Se desarrolló la planificación del proyecto científico que se va a realizar, la definición de los tiempos dedicados a cada actividad, los roles y responsabilidades en el proyecto.

C. Antecedentes y problemas.

En esta sección se desarrolló el enfoque del problema principal y también se elaboró las causas y los efectos del problema. Ésta sección es fundamental ya que después de esto se podrá formular el problema y realizar las respectivas preguntas del problema las cuales van a dar sustento de que el problema realmente existe.

D. Marco Teórico.

En el marco teórico se expone los antecedentes y las bases teóricas que le van a dar fundamento a este proyecto de investigación, el marco teórico está basado en referencias o citas de importantes personajes los cuales fortalecen el desarrollo del proyecto de investigación y de la misma manera está acompañado de un análisis realizado por parte del autor como reflexión a lo citado.

E. Planificación de la investigación.

Establece los mecanismos o pasos que se van a establecer para el desarrollo del proyecto de investigación.

F. Encuestas.

Para la planificación de las encuestas se desarrolló un pequeño formulario con preguntas específicas y claras el cual el experto deberá examinarlas y acorde a su experiencia y conocimiento las irá respondiendo, un aspecto fundamental en este proceso es que al finalizar el cuestionario se pregunte si está de acuerdo al proyecto de investigación y en caso de no estar de acuerdo que se debería mejorar o que cambios se debería de realizar.

G. Resultados y Análisis.

Con la información obtenida a través de los cuestionarios se realiza un análisis de las respuestas y en base a este análisis es factible realizar ciertos cambios que fortalezcan el proyecto de investigación o corroborar que el proyecto de investigación se está elaborando de manera correcta.

H. Plan de propuesta.

Es el desarrollo de lo que se ha propuesto en el proyecto de investigación, en esta sección se debe evidenciar los productos resultantes de la investigación.

I. Conclusiones y Recomendaciones.

Al final se desarrolla las conclusiones y recomendaciones las cuales indican los mecanismos más idóneos para el desarrollo del proyecto, se debe recomendar como desarrollar cada objetivo expuesto en el proyecto de investigación en inclusive se debe de citar alguna recomendación del experto en caso de que esta se haya realizado.

CAPÍTULO IV
ANÁLISIS Y RESULTADOS

4.1. Análisis de las Encuestas realizadas.

Para lograr constatar la validez de la investigación se han realizado las siguientes encuestas (Ver Anexo 10).

Pregunta 1.

Tabla 6: Encuesta aplicada a la pregunta 1.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera usted que la información es el activo más crítico que puede tener la organización?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	0	0%
	Totalmente de acuerdo.	4	100%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor

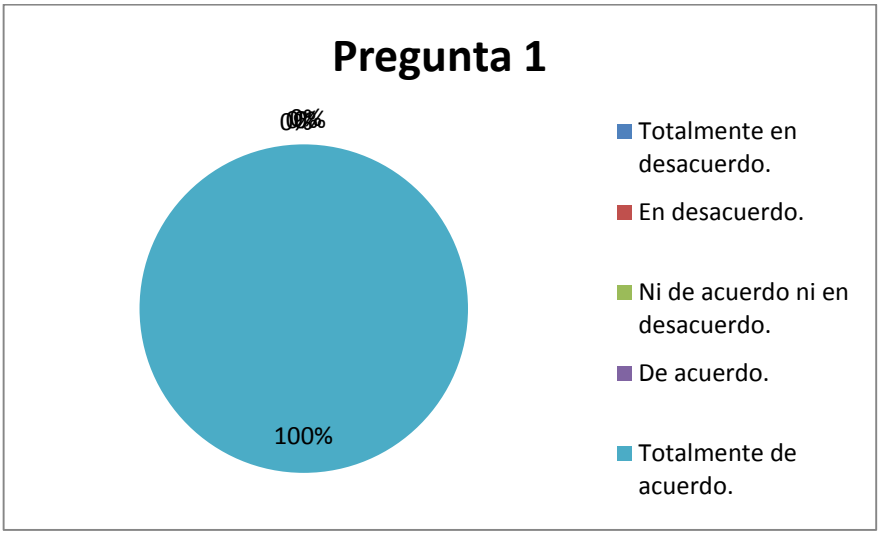


Figura 7: Gráfico estadístico de la pregunta 1.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor

Pregunta 2.

Tabla 7: Encuesta aplicada a la pregunta 2.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera usted que un Sistema de Gestión de Seguridad de la información va a ayudar a gestionar la información y los recursos informáticos de manera óptima y segura?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	1	25%
	Totalmente de acuerdo.	3	75%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor

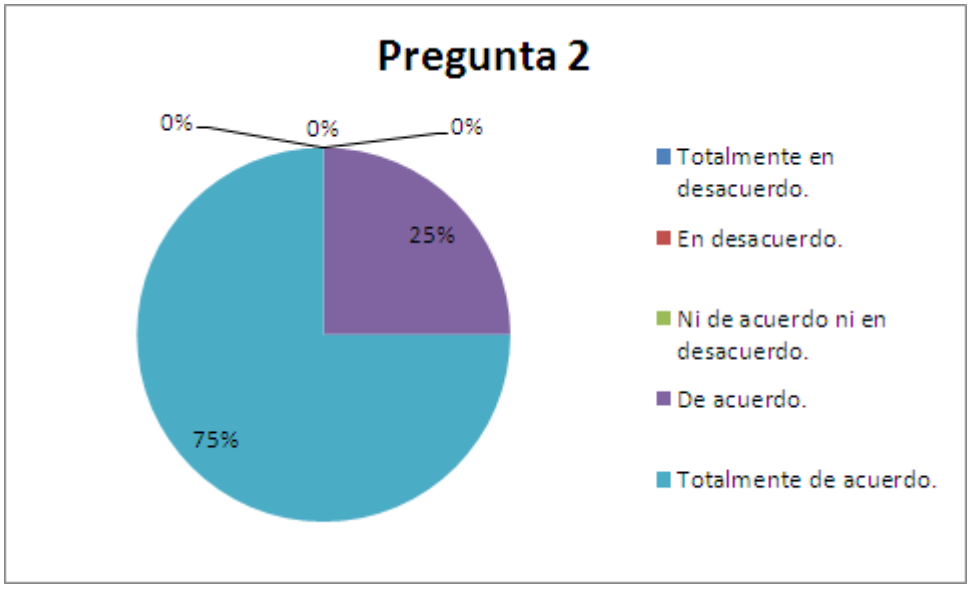


Figura 8: Gráfico estadístico de la pregunta 2

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor

Pregunta 3.

Tabla 8: Encuesta aplicada a la pregunta 3.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera usted que al diseñar de manera correcta un Sistema de Gestión de Seguridad de la información va a brindar un reconocimiento corporativo en el mercado?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	1	25%
	Totalmente de acuerdo.	3	75%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

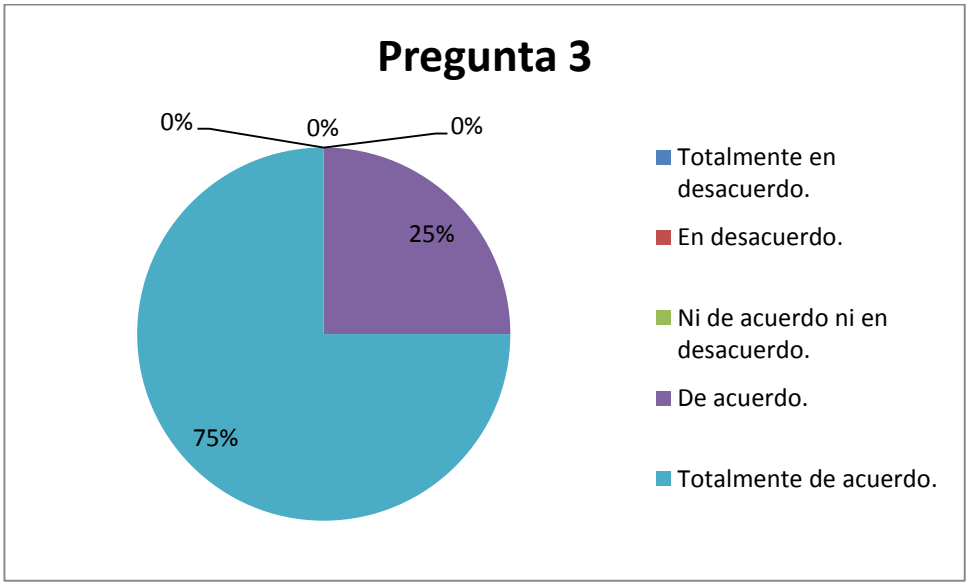


Figura 9: Gráfico estadístico de la pregunta 3.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 4.

Tabla 9: Encuesta aplicada a la pregunta 4.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera que aplicando el criterio de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011 va a garantizar los niveles de integridad, confidencialidad y disponibilidad de la información?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	2	50%
	Totalmente de acuerdo.	2	50%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

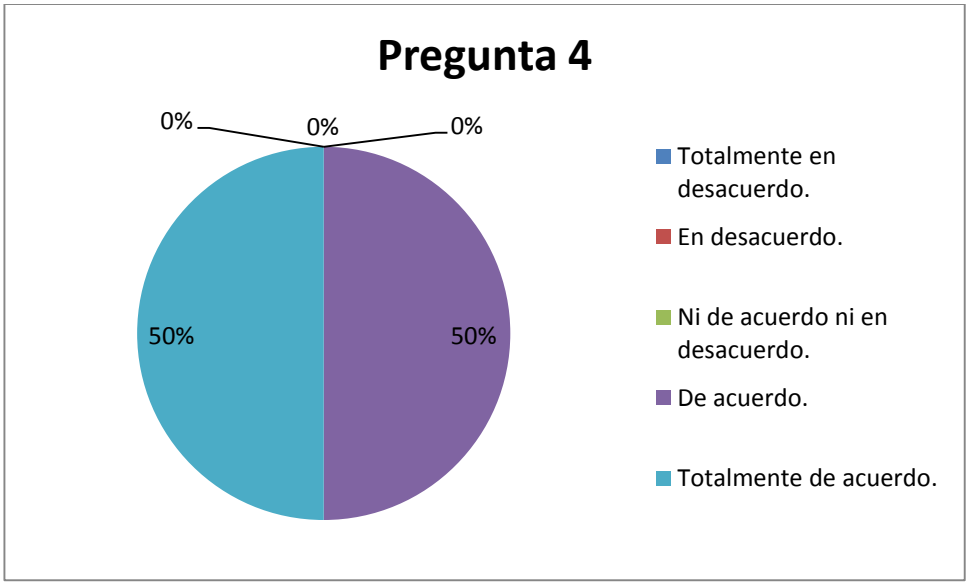


Figura 10: Gráfico estadístico de la pregunta 4.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 5.

Tabla 10: Encuesta aplicada a la pregunta 5.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cree usted que por medio de políticas de seguridad posible garantizar la seguridad de la información acorde a los requisitos del negocio?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	1	25%
	Totalmente de acuerdo.	3	75%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

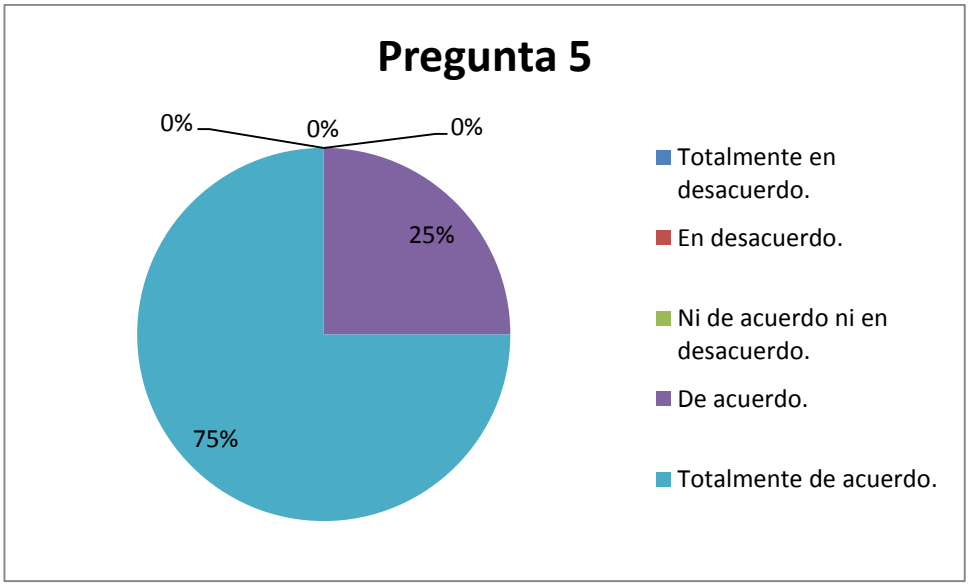


Figura 11: Gráfico estadístico de la pregunta 5.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 6.

Tabla 11: Encuesta aplicada a la pregunta 6.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cree usted que por medio de políticas de seguridad posible garantizar la seguridad de la información acorde a los requisitos del negocio?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	0	0%
	Totalmente de acuerdo.	4	100%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

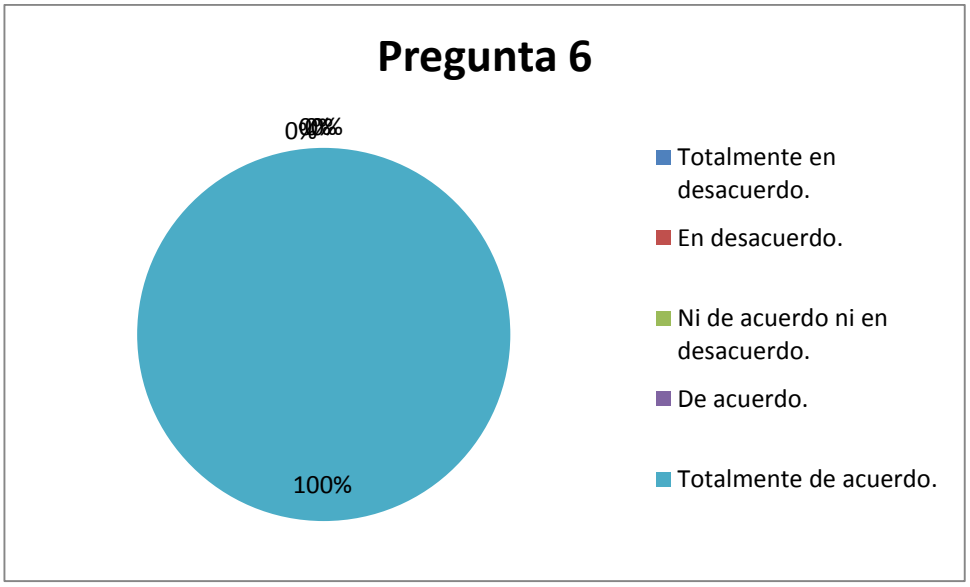


Figura 12: Gráfico estadístico de la pregunta 6.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 7.

Tabla 12: Encuesta aplicada a la pregunta 7.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera usted que una metodología de análisis de riesgo va a ayudar de gran manera a identificar y mitigar los posibles riesgos que existan dentro de su organización?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	0	0%
	Totalmente de acuerdo.	4	100%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

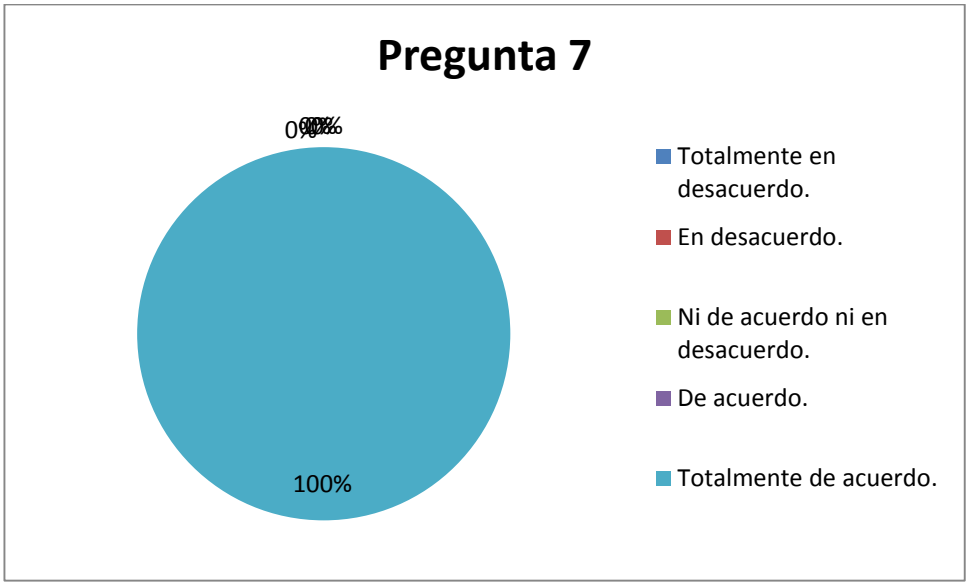


Figura 13: Gráfico estadístico de la pregunta 7.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 8.

Tabla 13: Encuesta aplicada a la pregunta 8.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cree usted que por medio de la evaluación de riesgos va a ser posible mitigar la mayor cantidad de vulnerabilidades existentes?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	2	50%
	Totalmente de acuerdo.	2	50%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

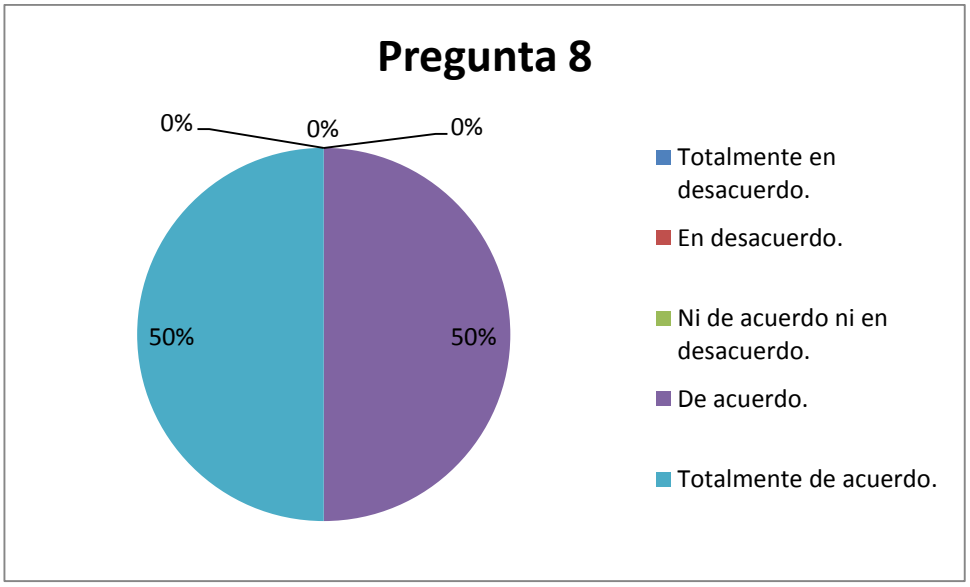


Figura 14: Gráfico estadístico de la pregunta 8.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 9.

Tabla 14: Encuesta aplicada a la pregunta 9.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Considera usted que los controles informáticos enunciados son necesarios en las organizaciones?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	1	25%
	Totalmente de acuerdo.	3	75%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

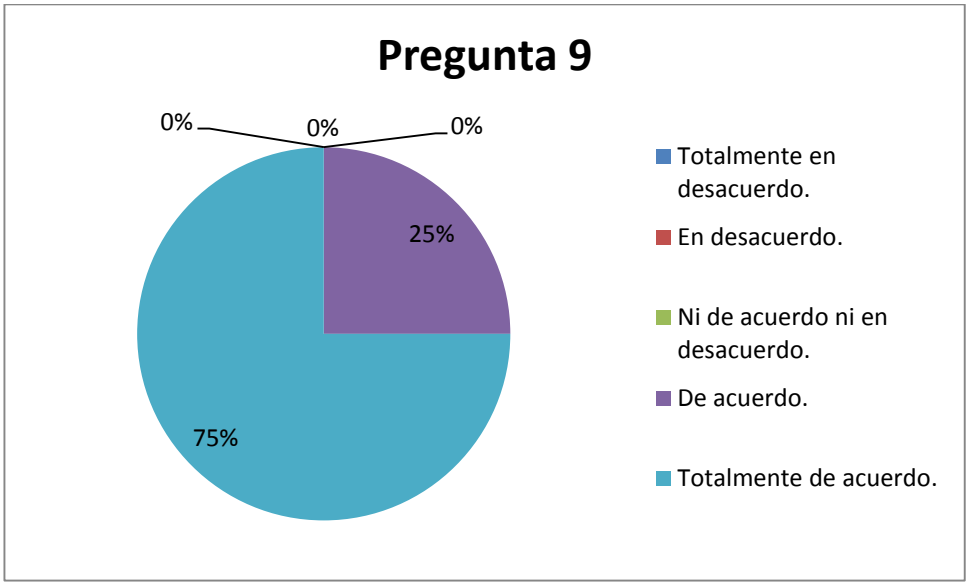


Figura 15: Gráfico estadístico de la pregunta 9.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

Pregunta 10.

Tabla 15: Encuesta aplicada a la pregunta 10.

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cree usted que es necesario que la organización efectúe el análisis y diseño de un SGSI, para preservar los activos informáticos?	Totalmente en desacuerdo.	0	0%
	En desacuerdo.	0	0%
	Ni de acuerdo ni en desacuerdo.	0	0%
	De acuerdo.	4	75%
	Totalmente de acuerdo.	1	25%

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

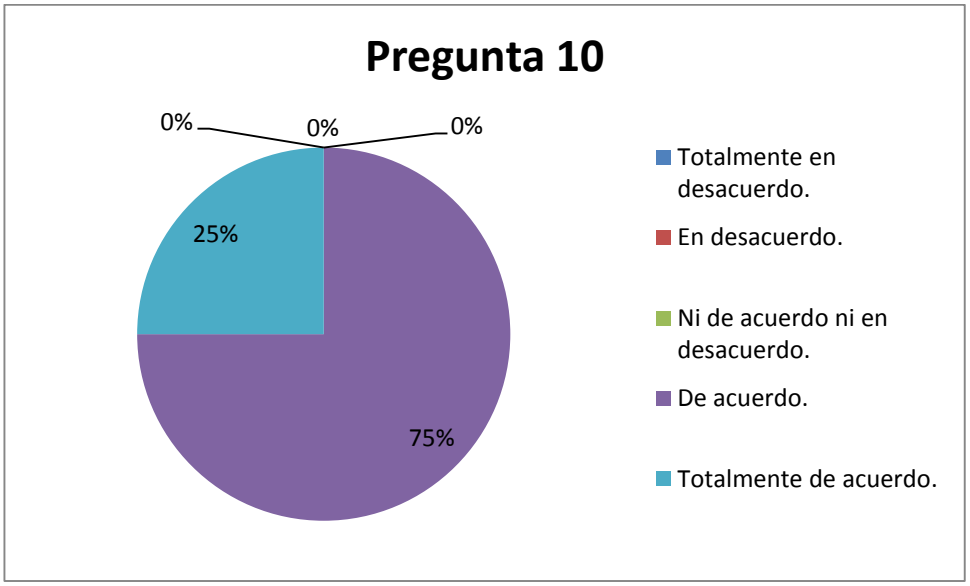


Figura 16: Gráfico estadístico de la pregunta 10.

Fuente: Datos de personas encuestadas que laboran en empresas del sector químico.

Elaborado por: Autor.

4.2. Interpretación de Datos y Verificación de Hipótesis.

Una vez concluidos los estudios de campo, que se apoyan principalmente en las encuestas realizadas en las principales empresas del sector químico del Ecuador, se han obtenido importantes conclusiones. Entre ellas se destacan:

i. El 100% de los encuestados considera que la información es el activo más crítico que puede tener la organización.

ii. El 75% de los encuestados considera que por medio de políticas de seguridad posible garantizar la seguridad de la información acorde a los requisitos del negocio.

iii. El 100% de los encuestados considera que con una metodología de análisis de riesgo va a ayudar de gran manera a identificar y mitigar los posibles riesgos que existan dentro de su organización.

iv. El 75% de los encuestados consideran que es necesario que la organización efectúe el análisis y diseño de un SGSI, para preservar los activos informáticos.

v. El 75% de los encuestados consideran que los controles informáticos enunciados son necesarios en las organizaciones.

vi. Al diseñar un Sistema de Gestión de Seguridad de la información basado en el criterio de la norma NTE INEN-ISO/IEC 27001:2011, se podrá garantizar los niveles de integridad, disponibilidad y confidencialidad de la información.

vii. Los procedimientos de seguridad y mecanismos de control, lograrán asegurar que los procesos de seguridad de la información se realicen de manera segura.

CAPÍTULO V
PROPUESTA.

5.1 Datos Informativos.

5.1.1 Análisis de las principales empresas dedicadas a la comercialización y distribución de productos químicos.

Tomando como fuente confiable la publicación realizada por la revista Vistazo la cual expone las principales empresas que se especializan en la comercialización y distribución de productos químicos del sector químico dentro de un ranking de 500 mayores empresas de diversos sectores en el Ecuador. Se tiene cuatro empresas principales tal como se muestra en la figura.

Figura 6: Principales Industrias Químicas del Ecuador.

Fuente: Superintendencia de Compañías, Servicio de Rentas Internas (SRI), Instituto Ecuatoriano de Seguridad Social (IESS) e información directa proporcionada por las empresas.

Elaborado por: Revista Vistazo.

Elaborando un análisis de esta fuente se puede considerar que la empresa que lidera el total de estas empresas es Ecuaquímica con un promedio de venta de $158'.685.000 comprendidos entre el año 2011 y 2012, por esta razón se encuentra clasificada en el puesto número 88 dentro de las 500 mayores empresas del Ecuador.

En la segunda posición se encuentra la empresa Brenntaq Ecuador, la cual tiene un promedio de ventas de $86'016.000, comprendidas entre el año 2011 y 2012, por esta razón ocupa la posición 180 dentro de las 500 mayores empresas del Ecuador.

En la tercera posición se encuentra la empresa Quimpac Ecuador, la cual tiene un promedio de ventas de $47'067.000, comprendidas entre el año 2011 y 2012, por esta razón ocupa la posición 314 dentro de las 500 mayores empresas del Ecuador.

En la cuarta posición se encuentra la empresa Química Industrial Montalvo Aguilar Quimasa, la cual tiene un promedio de ventas de $33'012.000, comprendidas entre el año 2011 y 2012, por esta razón ocupa la posición 468 dentro de las 500 mayores empresas del Ecuador.

5.1.2 Modelo de negocio de comercialización y distribución de químicos.

Las actividades de comercialización y distribución de productos químicos, se desarrollan según ordenanzas del plan regulatorio urbano de la ciudad de Guayaquil en zonas industriales, esto permite a las industrias grandes y de alto impacto la distribución y comercialización de sustancias químicas básicas, abonos, plaguicidas, entre otros.

Para tener de forma más clara el funcionamiento de este modelo de negocio a continuación se expone las principales características de las empresas dedicadas a la

comercialización y distribución de productos químicos, tomando la fuente de la revista Vistazo, tal como se muestra a continuación.

Las organizaciones se encuentran distribuidas a nivel nacional, por lo cual a continuación se exponen en la siguiente tabla, de manera estructural como se suelen establecer sus principales localidades.

Tabla 16: Principales oficinas de empresas del sector químico.

Empresa.	**Ciudad.**	**Dirección.**
Ecuaquímica.	Guayaquil.	Av. José Santiago Castillo y Av. Juan Tanca Marengo.
	Quito.	Av. 10 de Agosto N. 6090 y Av. Gaspar Villarroel.
	Ambato.	Av. Principal y vía Baños Km 2.5
	Cuenca.	Av. España N1409 y Turuhuaico.
Brenntaq Ecuador.	Guayaquil.	Vía Daule Km. 9 ½
	Quito.	Calle de los Cerezos y Panamericana Norte Km. 5 ½
	Ambato.	Ave. Indoamérica S/N, Sector Ingahurco Bajo, Km. 1.5
	Cuenca.	Parque Industrial, Ave. Carlos Tosi 305 y 2da transversal
Quimpac Ecuador.	Guayaquil.	Av. Rosavín y Calle Cobre Parque Industrial Ecuatoriano Km. 16,5, Vía a Daule.
	Quito.	Panamericana Sur Km 14 1/2, Parque Industrial Sur Lote 180.

	Ambato.	No dispone de oficinas en Ambato.
	Cuenca.	No dispone de oficinas en Cuenca.
Quimasa.	Guayaquil.	Km 11 1/2 Vía Daule Parque Industrial INMACOMSA entre Calle Teca y Gama
	Quito.	Av. Reina Victoria N 26-50 y la Pinta
	Ambato.	Parque Industrial Ambato 3ra etapa calle 4 No 50 intersección F
	Cuenca.	Panamericana Km 2,5 sector Narancay Bajo

Fuente: Datos obtenidos por medio del sitio web de las organizaciones.

Elaborado por: Autor.

5.1.3 Análisis de los principales productos de comercialización y distribución.

A continuación se exponen los principales productos de comercialización y distribución por las principales empresas del sector químico.

Tabla 17: Principales productos de empresas del sector químico.

Empresa.	**Productos.**	**Detalle.**
Ecuaquímica.	Agrícolas.	Distribuye y comercializa insecticidas, control de maleza, control de enfermedades, semillas certificadas, etc.
	Veterinarios.	Distribuye y comercializa suplementos minerales, antiparasitario externo, complejos vitamínicos, antibióticos, desinfectantes, bioestimulantes, entre otros.
	Acuícolas.	Se distribuye y comercializa prebióticos, suplementos vitamínico mineral, estimulante de fertilización.
	Higiene.	Se distribuye y comercializa productos para el control de todo tipo de plagas.
Brenntaq Ecuador.	Agrícolas tradicionales	Se distribuye y comercializa AGROFEED mezclas tradicionales (Agrofeed 10-30-10, Agrofeed 15-15-15, entre otros).
	Agrícolas especializadas.	Se distribuye y comercializa AGROFEED mezclas especializadas (Agrofeed Banano Completo, Agrofeed Palma, entre otros).
	Productos Simples Tradicionales.	Se distribuye y comercializa Nitrato de Amonio, Murato de Potasion, entre otros.

	KEMIRA.	Se distribuye y comercializa Mágnum P-44, Kemistar azul, Nitrato de calcio, entre otros.
Quimpac Ecuador.	Agrícola.	Se distribuye y comercializa Ácido Fosfórico.
	Alimenticio.	Se distribuye y comercializa Lecitina de Soya, Metabisulfito de Sodio, Metasilicato de Sodio, Parafina, Propilenglicol, entre otros.
	Acuicultura.	Se distribuye y comercializa Cloro Gas, Hipoclorito de Sodio, Metabisulfito de Sodio, Tripolisofato de Sodio, entre otros.
	Nutrición Animal.	Se distribuye y comercializa Bicarbonato de Sodio, Fosfato Bicálcico, Hipoclorito de Calcio, Sulfato de Cobre, entre otros.
Quimasa.	Agrícola.	Se distribuye y comercializa fertilizantes comunes y especiales (ácidos, sulfatos, nitratos, entre otros.)
	Alimenticia.	Se distribuye y comercializa preservantes, reguladores de PH, edulcorantes y saborizantes, entre otros.
	Industrial.	Se distribuye y comercializa pigmentos, solventes, tratamiento de aguas, tensoactivos.
	Veterinaria.	Se distribuye y comercializa antibacterianos, antiinflamatorios, antibióticos, aminoácidos, entre otros.

Fuente: Datos obtenidos por medio del sitio web de las organizaciones.

Elaborado por: Autor.

5.1.4 Procesos de comercialización y distribución de productos químicos.

Dado a que las empresas expuestas anteriormente tienen en común el mismo modelo de negocio, se ha tomado como referencia los procesos de comercialización y distribución de la empresa Ecuaquímica S.A., de tal manera que se pueda exponer de forma estándar, como se muestra a continuación.

a) Planificación de la producción bimensual.

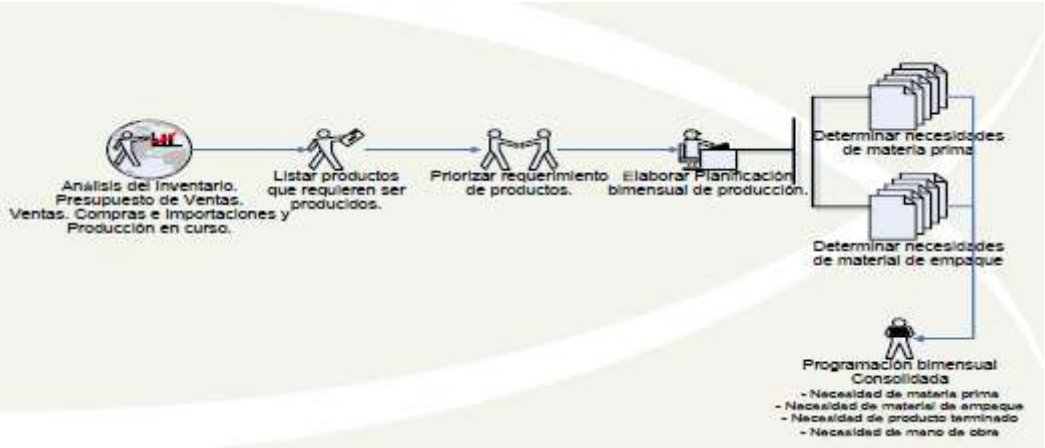


Figura 17: Planificación bimensual de producción.

Fuente: (Ecuaquímica S.A., 2014).

b) Planificación de la producción semanal.

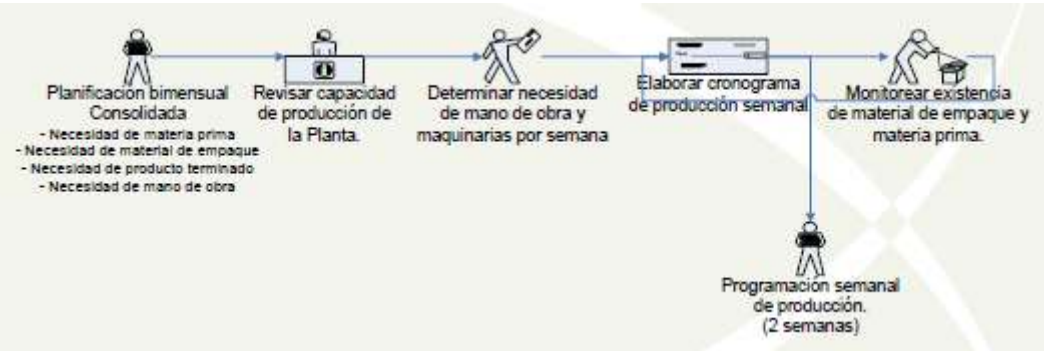


Figura 18: Planificación de producción semanal.

Fuente: (Ecuaquímica S.A., 2014).

c) Producción de la mercadería.

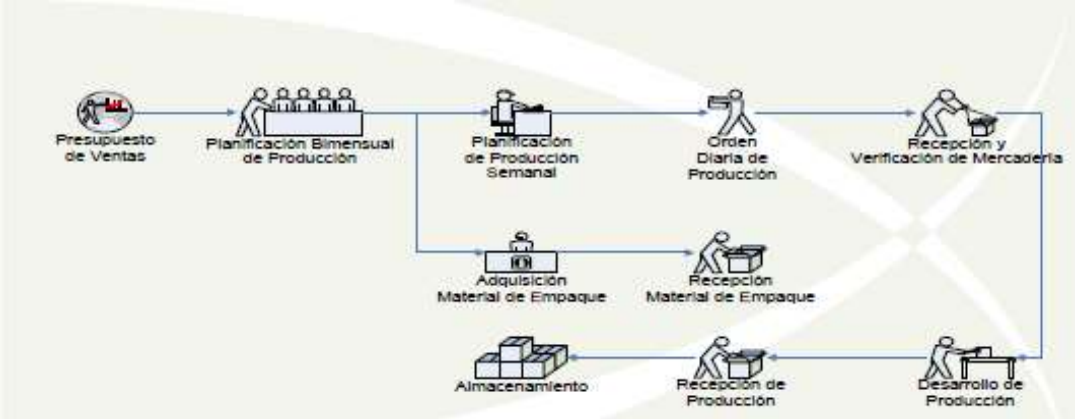


Figura 19: Producción de mercadería.

Fuente: (Ecuaquímica S.A., 2014).

.

d) Recepción y Verificación de mercadería.

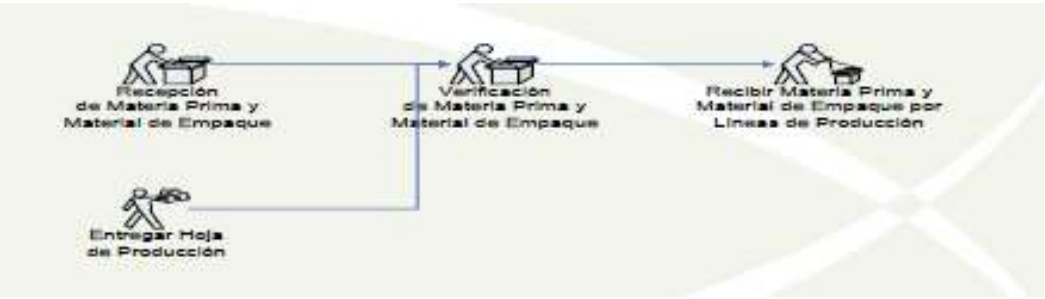


Figura 20: Recepción y verificación de mercadería.

Fuente: (Ecuaquímica S.A., 2014).

e) **Orden diaria de producción.**

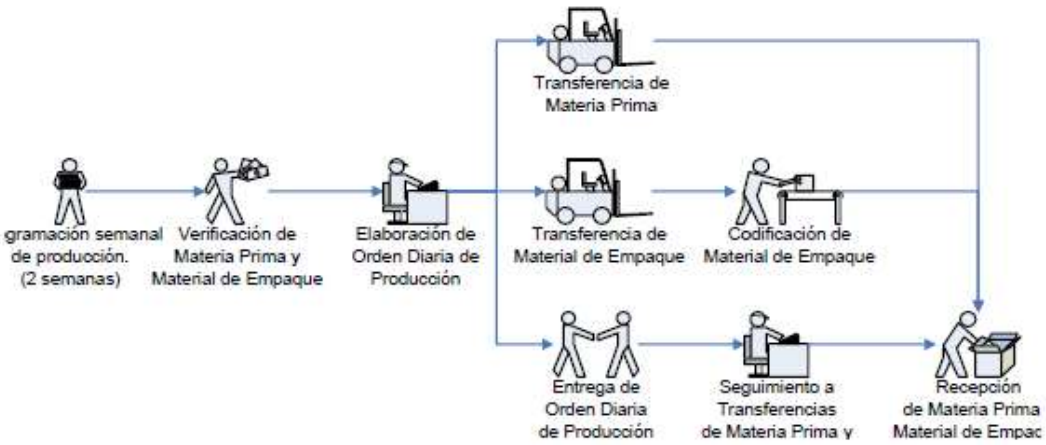


Figura 21: Producción diaria.

Fuente: (Ecuaquímica S.A., 2014).

f) Recepción de la producción.

Figura 22: Producción de mercadería.

Fuente: (Ecuaquímica S.A., 2014).

.

5.1.5 Exportación de productos químicos.

A continuación se expone el siguiente análisis realizado a la comercialización y distribución de productos químicos de Ecuador realizado por CORPEI.

Las exportaciones de diversos productos del sector químico, en su mayoría se representan entre el 30% y el 33% de las exportaciones del sector respectivamente, tal como se muestra a continuación.

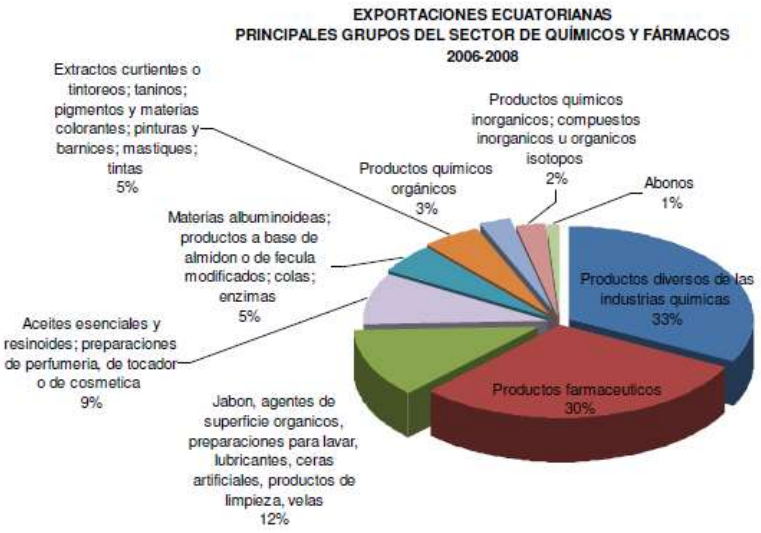


Figura 23: Exportaciones ecuatorianas (Principales grupos del sector químico.)
Fuente: (BCE/SIM (CORPEI), 2010).

Ecuador exporta productos químicos a más de 50 países en el mundo, en su mayoría son realizadas a países de Sudamérica, sin embargo países como Estados Unidos y Panamá también reciben valores significativos de estas exportaciones, tal como se muestra a continuación.

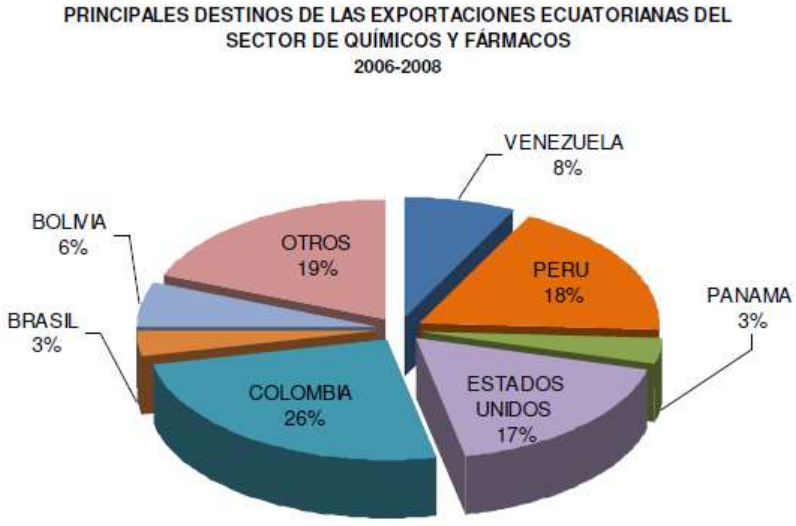


Figura 24: Principales destinos de exportaciones ecuatorianas.

Fuente: (BCE/SIM (CORPEI), 2010).

5.2 Antecedentes de la propuesta.

A continuación se expone el siguiente análisis realizado por la empresa líder en seguridad informática FireEye, el cual muestra un informe referente a un análisis estadístico de amenazas avanzadas para América Latina las cuales se encuentran dirigidas a redes de computadoras en América Latina durante el primer semestre del año 2014.

Acorde al Director de FireEye de Latino América Robert C. Freeman (2015), indica que "América Latina es un objetivo prioritario para los hackers que tratan de obtener información con respecto a tecnologías propietarias, procesos y precios que podrían ofrecer una ventaja en las transacciones de negocio", por lo tanto, acorde a lo indicado se expone lo siguiente.

Los principales actores o involucrados en realizar estas amenazas son motivados por objetivos financieros, políticos y sociales. Por lo cual el Informe Regional de Amenazas Avanzada, indica que "están explotando vulnerabilidades con mecanismos o métodos cada vez más sofisticados para lograr hurtar propiedad intelectual que es de carácter confidencial, información privada, información personal y otros datos que pueden ser generales beneficios económicos" (FireEye, 2014). Por lo tanto se podría indicar que estas violaciones ponen en alto riesgo tanto a personas como a las organizaciones de consecuencias financieras, legales y de reputación.

Infecciones Específicas en el Vertical de la industria.

Acorde al estudio realizado por FireEye, en el cual se exponen los eventos o incidentes de seguridad que afectan a las organizaciones latinoamericanas, en el

mismo se puede evidenciar que Los Químicos/Manufactura/Minería constituyen casi la mitad de todas las incidencias reportadas.

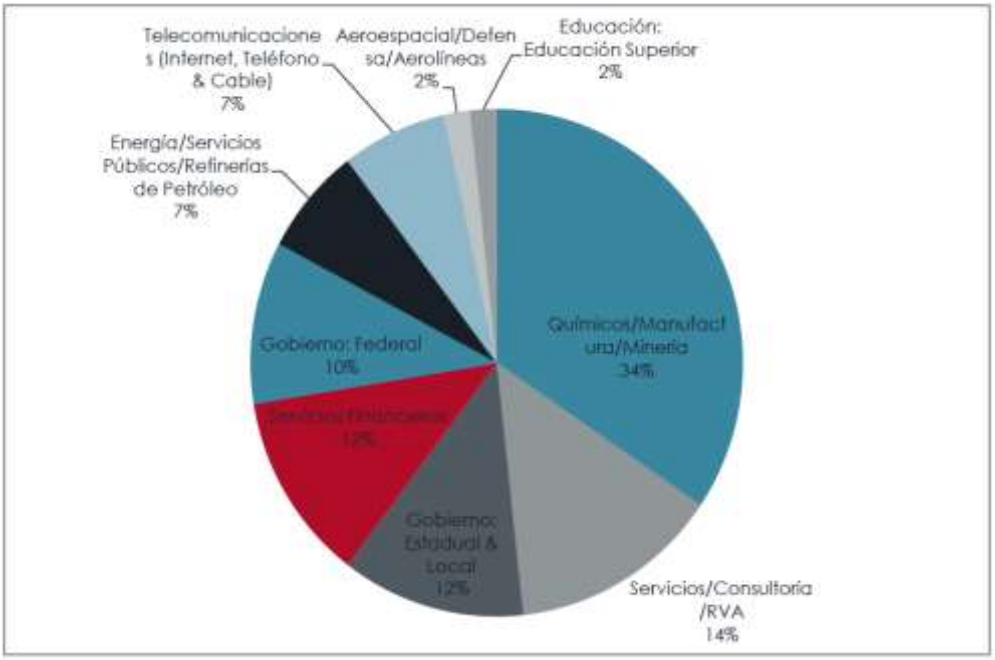


Figura 25: Eventos de Seguridad por industria que afectan a Latino América.

Fuente: (FireEye, 2014).

De manera adicional, se ha realizado el análisis del siguiente gráfico (Figura 26) que de forma comparativa se muestra los eventos de seguridad en América Latina, en comparación los verticales a nivel mundial. En el gráfico se puede evidenciar que las industrias de Químicos, Manufactura y Minería, se encuentran de manera desproporcionada en América Latina por motivo de que la industria es su principal motor estratégico de la región. Es muy probable que los involucrados en realizar estas amenazas estén enfocándose en este sector con el objetivo de adquirir información referente a procesos de negocio (fórmulas, compuestos, etc.), tecnologías patentadas, ventajas competitivas, etc.

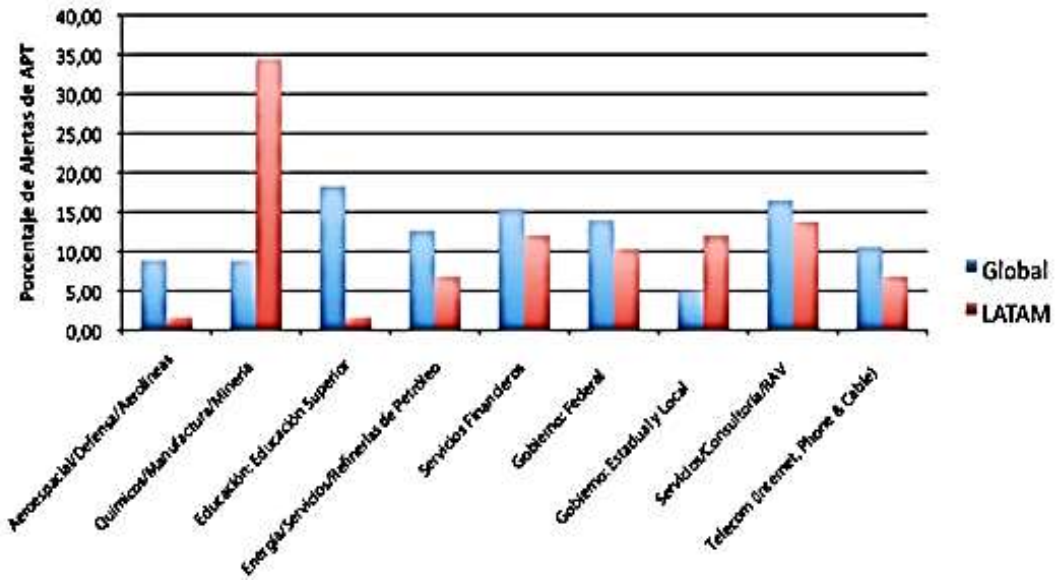


Figura 26: Eventos de seguridad detectados en Latinoamérica y el resto del mundo.

Fuente: (FireEye, 2014).

En el desarrollo del diseño de un Sistema de Gestión de Seguridad de la información va a ser posible mitigar la mayoría de estas vulnerabilidades y riesgos de tal manera que se podrá garantizar los niveles apropiados de integridad, disponibilidad y confidencialidad y de la misma forma gestionar la información de manera óptima y segura.

5.3 Justificación.

Los principales justificativos para este proyecto son:

- Garantizar los principios de seguridad de la información, con el objetivo de evitar las siguientes amenazas.
    - Alteración de la información.
    - Robo de la información.
    - Pérdida de la Información.
    - Falta de disponibilidad en la información.

- Solventar vulnerabilidades y mitigar riesgos en los sistemas que afectan a la seguridad de la información.
- Contribuir a que los procesos de comercialización y distribución se realicen de manera segura.
- Reconocimiento corporativo dentro del mercado nacional como internacional.
- La apertura de nuevas oportunidades de mercado, tanto de nivel local como internacional, al conocer que el sector es más seguro.

5.4 Objetivos.

Diseñar un Sistema de Gestión de Seguridad de la Información, que sirva como lineamiento de seguridad y mejora continua para un modelo de negocio dedicado a la comercialización y distribución de productos químicos.

5.5 Análisis de Factibilidad.

A continuación expone que con una inversión considerablemente modesta en el transcurso de seis meses se logrará alcanzar lo siguiente.

5.5.1 Cronograma general de la propuesta.

Acorde a lo expuesto anteriormente se ha desarrollado el siguiente diagrama de Gantt (Figura 27), con el objeto de visualizar el tiempo estimado de este proyecto de una manera más detallada.

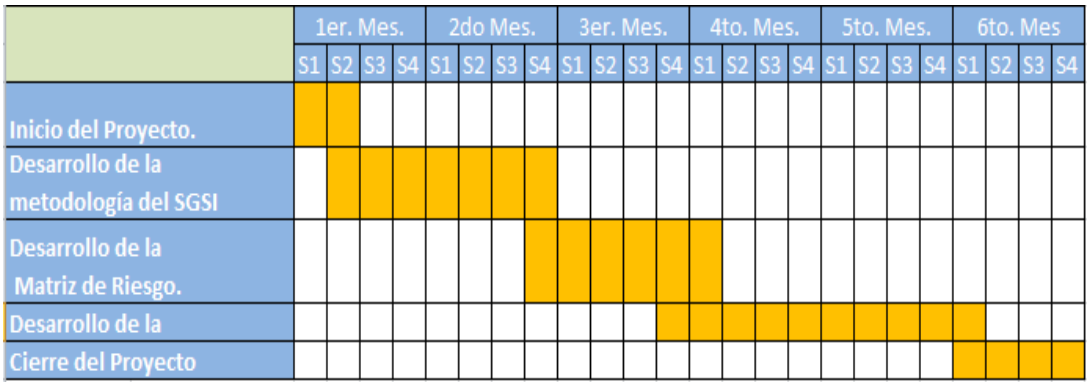


Figura 27: Diagrama de Gantt, detallando las actividades de la propuesta.

Fuente: Autor.

5.5.2 Oferta Económica.

En base al requerimiento expuesto en este proyecto de investigación, los servicios tendrán un periodo de duración de 24 semanas de trabajo, para las actividades indicadas y según el cronograma general presentado.

Acorde a los servicios proporcionados en esta propuesta a continuación se detalla los siguientes valores.

A. Desarrollo de la Metodología del SGSI.

Tabla 18: Costo de la Etapa 2 de la propuesta.

Servicios.	Precio US$ (Sin IVA)
Para esta etapa del proyecto se detalla el siguiente alcance. • Desarrollar la declaración documentada de la política, se estará cumpliendo con el punto 4.3.1a) de la norma, para el correcto diseño del SGSI. • Desarrollar el alcance del SGSI, según el apartado 4.3.1b) de la norma. • Desarrollar una descripción de la metodología de evaluación de riesgo, según el apartado 4.3.1d) de la norma.	**$ 6.000,00**

• Desarrollar un plan de tratamiento de riesgos estándar, según el apartado 4.3.1d) y 4.3.1e) de la norma • Elaborar la declaración de aplicabilidad estándar, según el apartado 4.3.1j).	
Total del Servicio.	**$ 6.000,00**

Fuente: Autor.

B. Desarrollo de la Matriz de Riesgo.

Tabla 19: Costo de la Etapa 3 de la propuesta.

Servicios.	Precio US$ (Sin IVA)
Para esta etapa del proyecto se detalla el siguiente alcance. • El desarrollo de la Matriz de Riesgo.	**$ 3.000,00**
Total del Servicio.	**$ 3.000,00**

Fuente: Realizado por el autor de este proyecto.

C. Desarrollo de la Declaración de Aplicabilidad.

Tabla 20: Costo de la Etapa 4 de la propuesta.

Servicios.	Precio US$ (Sin IVA)
Para esta etapa del proyecto se detalla el siguiente alcance. • Desarrollo de la Declaración de Aplicabilidad.	**$ 4.000,00**
Total del Servicio.	**$ 4.000,00**

Fuente: Autor.

Costo total de la propuesta.

Tabla 21: Costo del proyecto en general

Servicios.	Precio US$ (Sin IVA)
Servicios de consultoría correspondiente a lo siguiente. • **Levantamiento de información para la ejecución de la Fase I y Fase II del proyecto.** • **Ejecución de la Fase I, Fase II, Fase III, Fase IV y Fase V.**	**$ 13.000,00**
Total del Servicio (A+B+C).	**$ 13.000,00**

Fuente: Autor.

5.6. Fundamentación.

Para llegar a garantizar que la información es gestionada de manera correcta y segura es necesario identificar inicialmente su periodo o ciclo de vida, así mismo los aspectos más importantes acogidos para garantizar la disponibilidad, integridad y confidencialidad, la cual se expone a continuación.

- **Confidencialidad:** La información no se expone, ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** El mantenimiento de la fidelidad y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** El acceso y uso de la información y los sistemas, por parte de individuos, entidades o procesos autorizados cuando estos lo requieran.

Acorde al conocimiento del ciclo de vida de cada información relevante es necesario adoptar la utilización de un proceso sistemático, documentado y conocido por toda la

organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información.

5.7. Modelo Operativo.

5.7.1. Análisis del SGSI para un modelo de negocio de comercialización y distribución de productos químicos.

Con el objetivo de robustecer la factibilidad del diseño de un Sistema de Gestión de Seguridad de la información se han realizado los siguientes análisis.

5.7.1.1. Análisis PESTEL para el diseño del SGSI.

Se ha desarrollado este análisis con el objetivo de captar con precisión las implicaciones que tiene el diseño de un SGSI en las organizaciones con un modelo de negocio aplicado a la comercialización y distribución de productos químicos, en diversos ambientes como político, económico, social, tecnológico, legislativo y ecológico, por lo tanto acorde a lo indicado anteriormente se expone lo siguiente.

Tabla 22: Análisis PESTEL del diseño del SGSI.

Político.	**Económico.**	**Social.**
• Cambios y aplicación de nuevas disposiciones o procesos regulatorios relacionados con el modelo de negocio de la organización, pueden llegar a dificultar la implementación del SGSI.	• Cambios y aplicación de nuevos impuestos pueden afectar en la aplicación de controles de seguridad, lo cual puede llegar a retrasar la implementación del SGSI.	• Imagen corporativa, da confianza a los proveedores y consumidores.

Tecnología.	**Legislación.**	**Ecológico.**
• La implementación del SGSI brinda a la organización una estrategia competitiva que da como resultado una diferencia importante en el mercado.	• Los empleados son conscientes que existe una política interna de la organización la cual por su incumplimiento pueden llegar a ser sancionados dependiendo de la gravedad de la contravención.	• Expone una tendencia con el uso correcto de la información, que esta se encuentre de manera digital para mantenerse más segura y solo sea expuesta físicamente por procedimientos óptimos y seguros, lo cual disminuye el uso del papel.

Fuente: Autor.

De la misma manera se ha realizado el siguiente análisis FODA de tal manera de que se pueda demostrar todas las ventajas y dificultades que se podría tener en el transcurso del desarrollo de este proyecto.

5.7.1.2. Análisis FODA para el diseño del SGSI.

Se ha desarrollado este análisis con el objetivo de indicar el balance estratégico que tendría el diseño de un SGSI para un modelo de negocio dedicado a la comercialización y distribución de productos químicos, esto implica las fortalezas, debilidades, oportunidades y amenazas, por lo tanto de acuerdo a lo expresado anteriormente se expone lo siguiente.

Tabla 23: Análisis FODA del diseño del SGSI

Fortalezas.	**Debilidades.**
• Uso correcto de los recursos informáticos. • Reducción de riesgos que afecten la disponibilidad, integridad y confiabilidad de la información. • Uso consiente de la información.	• Resultados a medio o largo plazo. • Ausencia de conocimiento de la normativa. • Costos elevados al aplicar los controles de seguridad apropiados.
Oportunidades.	**Amenazas.**
• Obtener la certificación NTE INEN-ISO/IEC 27001:2011. • Alinear la tecnología de información con el modelo del negocio. • Mejora la calidad dentro de la organización.	• Oposición interna al aplicar los controles o mecanismos de seguridad apropiados.

Fuente: Autor.

Para desarrollar el diseño de un Sistema de Gestión de Seguridad de la Información es conveniente realizar de forma inicial un levantamiento de información con el objetivo de distribuir de manera correcta los tiempos y tareas que se van a realizar. De la misma forma para tener una idea del estado actual de la organización y que estrategias se pueden realizar para la obtención de objetivos futuros, se hace necesario el siguiente análisis.

5.7.1.3. Análisis de Brechas.

Por medio de este análisis se va a lograr identificar la situación actual referente a la gestión de la seguridad de la información dentro del modelo de negocio dedicado a la comercialización y distribución de productos químicos.

Para realizar este análisis se puede utilizar una plantilla (Ver Anexo 1), con el objetivo de que se pueda evaluar el cumplimiento de todas las directrices y objetivos de control que se encuentran requeridos por la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2001.

Del resultado obtenido se generan estrategias y mecanismos de acción para el cumplimiento de los procedimientos y objetivos de control que se indican en la normativa anteriormente mencionada, y con esto llegar a desarrollar el Sistema de Gestión de Seguridad de la información.

5.7.2. Diseño de un Sistema de Gestión de Seguridad de la Información.

5.7.2.1. Manual de Gestión de Seguridad de la Información.

Los componentes principales del Manual de Gestión de Seguridad de la Información, según el apartado 4.3.1 del criterio de la norma NTE INEN-ISO/IEC 27001:2001, son los siguientes.

- El alcance del SGSI.
- Declaración documentada de la política.
- Descripción de la metodología de evaluación de riesgos.
- La declaración de aplicabilidad.

El Manual del Sistema de Gestión de Seguridad de la información se encuentra desarrollado en el Anexo 2.

A continuación se expone cada uno de los componentes principales del Sistema de Gestión de Seguridad de la Información de manera detallada, tal como lo requiere el apartado 4.3.1 de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011.

a) Alcance del SGSI.

El alcance y los límites del SGSI son términos de las características de la actividad empresarial, del modelo de negocio, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier exclusión del alcance.

El alcance del SGSI indica que sobre los procesos de comercialización y distribución de productos químicos se va a aplicar las políticas, procedimientos de seguridad, controles, etc.

El alcance del SGSI encuentra desarrollado en el capítulo 2 del anexo 2.

b) Declaración documentada de la política.

En la política se incluye un marco para la fijación de objetivos y se establece una orientación general sobre las directrices y principios de actualización en relación con la seguridad de la información.

Se ha tomado en cuenta los requisitos de la actividad empresarial, los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales.

Se encuentra alineada con el contexto de la estrategia de gestión de riesgos de la organización contexto en el que tendrá lugar la creación y el mantenimiento del SGSI.

La declaración documentada de la política se lo puede encontrar desarrollado en el capítulo 5 del Anexo 2.

c) Descripción de la metodología de evaluación de riesgos.

Se ha utilizado MAGERIT como metodología de gestión de riesgo, la cual busca un método aproximado para el análisis y evaluación de riesgos así como para la gestión de seguridad.

La metodología de evaluación de riesgos contiene.

- Identificación de activos.
- Clasificación de activos.
- Identificación de amenazas
- Clasificación de amenazas
- Potencialidad de ocurrencia.
- Identificación de Impactos.
- Clasificación de Impactos.

La metodología de evaluación de riesgo se lo puede encontrar desarrollado en el Anexo 2, capítulo 6.

d) La declaración de aplicabilidad.

La declaración de aplicabilidad es un documento que contiene todos los controles utilizados, esto se lo se puede revisar de manera más detallada en el anexo 3, donde se encuentra desarrollado el documento declaración de aplicabilidad.

Este documento contiene.

- Los objetivos de control y los controles seleccionados con su respectiva justificación de su selección.
- Lo objetivos de control y controles actualmente implementados.
- Las exclusiones de cualquier objetivo de control y controles del anexo A. así como la justificación de estas exclusiones.

e) Procedimientos y mecanismos de control que soportan el SGSI.

Se debe de mejorar de manera continua la eficacia de un SGSI, mediante el uso de la política, los objetivos de seguridad de la información, las auditorías, las acciones correctivas, preventivas y de las revisiones por parte de dirección.

Por esta razón como parte de los procedimientos que soportan el SGSI se han elaborado los siguientes procedimientos de una manera estándar.

i. Control de Documentos y Registros (Ver Anexo 4).
ii. Auditorías Internas (Ver Anexo 5).
iii. Revisión por la dirección (Ver Anexo 6).
iv. Acciones correctivas y preventivas (Ver Anexo 7).

v. Metodología de análisis y evaluación de riesgos (Ver Anexo 8).

f) Informe de evaluación de riesgos.

Se ha desarrollado un informe de evaluación de riesgo de tal forma que se pueda evidenciar las amenazas identificadas, la eficacia de controles implementados y de la misma manera se ha definido los niveles aceptables de un riesgo encontrado.

De manera más detallada se puede revisar el Anexo 9, donde se encuentra desarrollado la Matriz de Evaluación y Análisis de riesgos.

g) Registros requeridos por la norma.

Como parte de los principales registros que son requeridos por la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011, se han elaborado los siguientes de una manera estándar.

i. Control de Documentos y Registros (Ver Anexo 4, cap. 6).
ii. Auditorías Internas (Ver Anexo 5, cap. 8).
iii. Acciones correctivas y preventivas (Ver Anexo 7, cap. 6).
iv. Informe de análisis y evaluación de riesgos (Ver Anexo 9).

5.8. Metodología.

Etapas del Proyecto.

A partir del enfoque propuesto, y utilizando la metodología para la gestión de proyecto, se ha definido un proyecto compuesto por 5 fases que se muestran gráficamente a continuación.

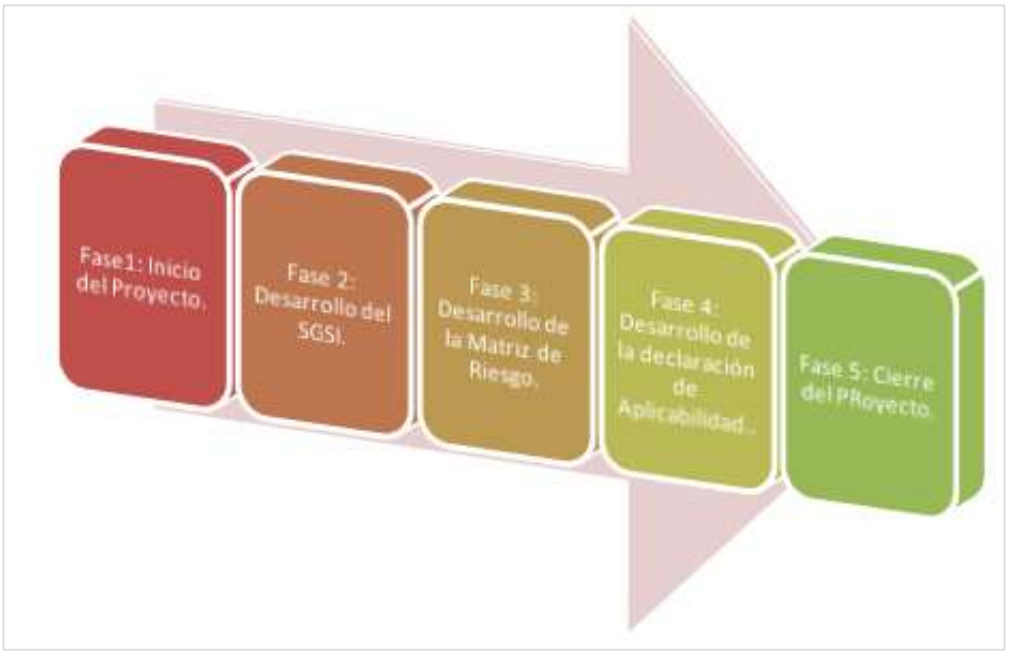


Figura 28: Fases del diseño de Gestión de Seguridad de la Información.

Fuente: Autor.

Actividades a realizarse en cada etapa.

A continuación se detalla para cada una de las etapas del proyecto, las actividades que se llevarán a cabo, la información que se necesitará que se provea, y los entregables que se presentarán como resultado del desarrollo de la etapa.

Fase 1: Inicio del Proyecto.

Esta primera etapa consiste en identificar los roles y perfiles del personal que participa en el proyecto, planificar las actividades a desarrollar, validar plazos de entrega, asignar responsabilidades al interior del equipo, y comunicar los mecanismos de gerenciamiento.

Tabla 24: Detalle de las actividades en la Fase 1 de la propuesta.

<table>
<tr><th>Actividades.</th><th>Información requerida.</th></tr>
<tr><td rowspan="2">• Entregar la solicitud de información requerida para la ejecución del proyecto.
• Definir plan de trabajo y cronograma en conjunto con el cliente.
--
• Presentar el plan de Gerenciamiento del proyecto.
• Presentar el cronograma detallado de actividades del proyecto.
• Realizar la sesión de inicio (Kick-off), incluyendo una reunión inicial definiendo lo siguiente.
o Objetivo y alcance del proyecto.
o Metodología a emplearse.
o Cronograma general.</td><td>• Identificación del equipo de trabajo.</td></tr>
<tr><th>Entregables.</th></tr>
<tr><td></td><td>• Plan de Gerenciamiento del Proyecto.
• Cronograma de Actividades del Proyecto.</td></tr>
</table>

Fuente: Autor.

Fase 2: Desarrollo del SGSI.

Esta fase consiste en el desarrollo de la metodología para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) empleando el criterio de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011, sobre los procesos de mayor criticidad que se hayan identificado dentro de la organización, la misma que permitirá determinar el alcance dentro del SGSI (Sistema de Gestión de Seguridad de la Información) con sus respectivos controles y lineamientos de seguridad.

Tabla 25: Detalle de las actividades en la Fase 2 de la propuesta.

Actividades.	Información requerida.
• Desarrollar la declaración documentada de la política, se estará cumpliendo con el punto 4.3.1a) de la norma, para el correcto diseño del SGSI. • Desarrollar el alcance del SGSI, según el apartado 4.3.1b) de la norma. • Desarrollar una descripción de la metodología de evaluación de riesgo, según el apartado 4.3.1d) de la norma. • Desarrollar un plan de tratamiento de riesgos estándar, según el apartado 4.3.1d) y 4.3.1e) de la norma • Elaborar la declaración de aplicabilidad estándar, según el apartado 4.3.1j).	• Árbol de procesos de la organización. **Entregables.** • El documento Sistema de Gestión de Seguridad de la información con el desarrollo de los requisitos del apartado 4.3.1 de la norma técnica NTE INEN-ISO/IEC 27001:2011.

Fuente: Autor.

Fase 3: Desarrollo de la Matriz de Riesgo.

Esta fase consiste en el desarrollo de la metodología para la identificación de los riesgos, la evaluación del cumplimiento y la efectividad de los controles de seguridad ya existentes dentro de la organización, se realizará las debidas recomendaciones de cómo aplicar estos controles ya que esto conlleva en la mayoría de los casos la aplicación de nuevas soluciones de seguridad o la modificación en la configuración de estas soluciones dentro en la organización, lo que en algunos casos puede causar cambios drásticos a nivel de su infraestructura tecnológica.

Tabla 26: Detalle de las actividades en la Fase 3 de la propuesta.

Actividades.	Información requerida.
• Desarrollar una matriz de evaluación y análisis de riesgos y cumplimiento de los controles de seguridad que se van a aplicar.	• Documento Declaración de Aplicabilidad.
	Entregables.
	• Matriz de Análisis y Evaluación de Riesgos.

Fuente: Autor.

Fase 4: Desarrollo de la Declaración de Aplicabilidad.

Esta fase consiste en el desarrollo de la Declaración de Aplicabilidad el cual es un documento fundamental cuando se desea elaborar un SGSI (Sistema de Gestión de Seguridad de la Información) en una organización, el cual consiste en realizar un documento indicando los controles de seguridad a ser aplicados sobre los procesos identificados y con sus debidas exclusiones en caso de que existan.

Tabla 27: Detalle de las actividades en la Fase 4 de la propuesta.

Actividades.	Información requerida.
• Desarrollar del documento Declaración de Aplicabilidad.	• Matriz de Gestión de Riesgos. • Árbol de procesos de la organización.
	Entregables.
	• El documento Declaración de Aplicabilidad.

Fuente: Autor.

La elección de los controles es parte del Plan de Tratamiento de riesgos. Este documento busca plantear de una manera clara y efectiva de qué manera se va a implementar los controles, que área o departamento dentro de la organización se va a responsabilizar de ello, cuando se lo realizará y que costo tendrá.

Por lo tanto se podrá llegar a la conclusión que por medio de este documento se puede llegar a obtener un plan de acción para coordinar todas las actividades que se desarrollarán para el cumplimiento de los controles necesarios, los cuales se encuentran como uno de los principales requisitos para el proyecto de certificación de NTE INEN-ISO/IEC 27001:2011.

Observación: Se debe te tener en cuenta que si una organización desea llevar a cabo una Declaración de aplicabilidad y esta decide no aplicar ningún control de seguridad de los 133 controles definidos en la norma, esta entidad debe de poseer la capacidad de demostrar que ha realizado el análisis de riesgos respectivo, y ha llegado a la conclusión de no implantarlos. De la misma manera puede presentarse un escenario contrario, es decir, que ciertos o la mayor parte de los controles que se encuentran definidos en la norma ya estuviesen implementados previamente en la organización o que la entidad considere insuficientes los controles propuestos y tome la decisión de ampliarlos con el objetivo de garantizar aún más la seguridad de su información.

Fase 5: Cierre del Proyecto.

En la etapa final se realiza la presentación de los entregables finales y se cierran las actividades del proyecto.

Tabla 28: Detalle de las actividades en la Fase 5 de la propuesta.

Actividades.	**Información requerida.**
• Presentación de entregables. • Obtener la aceptación del patrocinador. • Realizar revisión tras cierre del proyecto.	• Listado de asistentes a la presentación ejecutiva de resultados del proyecto.
	Entregables.
	• Presentación del cierre del proyecto.

Fuente: Autor.

Después de la realización de las etapas definidas con anterioridad, la ejecución exitosa de este proyecto promete la obtención de los siguientes beneficios.

- Reducción de costos directamente relacionados con incidentes que afecten la seguridad de la información.
- Garantiza la ejecución de que los procesos de comercialización y distribución se realicen de manera segura.
- Nuevas oportunidades en el mercado a causa del incremento de los niveles de confianza ante clientes y alianzas estratégicas.
- Identificación apropiada y eficaz de riesgos, amenazas e impactos en la actividad empresarial.

5.9. Administración.

ePulpo es una herramienta que facilita la gestión del Sistema de Gestión de Seguridad de la Información de manera óptima y eficiente. Por esta razón se exponen los componentes principales de esta herramienta con el objetivo de optimizar la gestión del análisis y diseño de un Sistema de Gestión de Seguridad de la información.

a) Gestión Documental.

Se logrará documentar, almacenar, difundir y controlar el acceso a los siguientes componentes que forman parte del Sistema de Gestión de Seguridad de la Información.

- El alcance del SGSI.
- La Política de Seguridad.
- Los procedimientos y mecanismos de control de soportan el SGSI.
- La metodología de riesgo.
- La declaración de aplicabilidad.

Ir a Menú > Gestión Documental > Espacio Raíz > ISO 27001-SGSI, donde se logrará ver la estructura donde se almacena la documentación relativa del SGSI.

Otra forma es que por medio del menú principal de la herramienta se utilice un wizard, el cual ayudará a documentar los componentes del SGSI paso a paso, tal como se muestra a continuación.

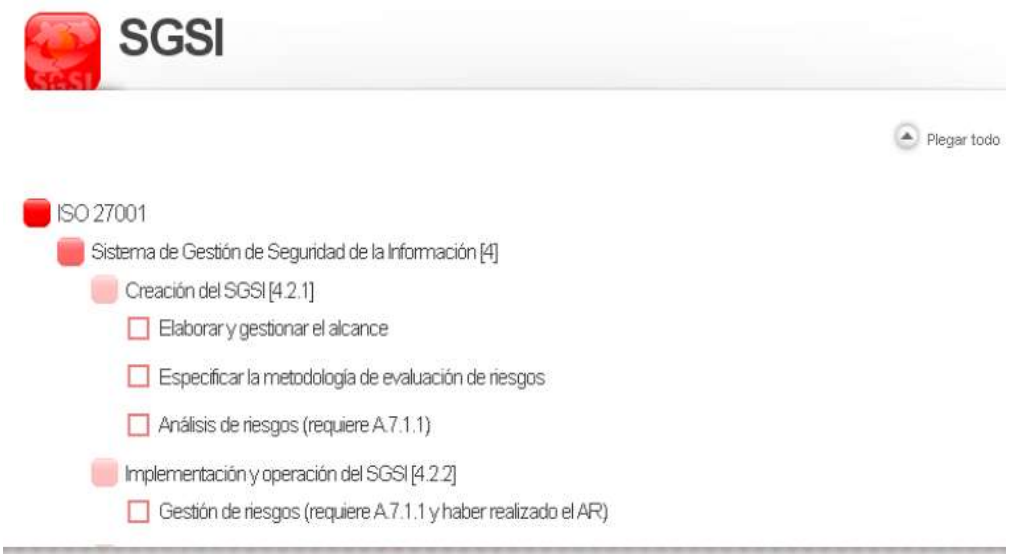


Figura 29: Gestión Documental (Wizard).

Fuente: Autor.

Dentro de las acciones que se pueden realizar en este componente se encuentran los siguientes.

- Crear y editar documentos en línea.
- Subir documentos via web o copiando estos a una carpeta.
- Control histórico de los documentos.
- Responsabilidad sobre documentos y procesos.
- Gestiona el acceso a documentación obsoleta.
- Dispone de un motor de flujo de trabajo para las siguientes operaciones.
    - Aprobación de documentos.
    - Creación de asistentes de tramitación.
    - Control de plazos.
    - Control de tareas.

A continuación se expone la siguiente imagen como muestra de la Gestión Documental (Figura 30) y acción la Aprobación y Difusión (Figura 31) como parte del motor de flujo que tiene la herramienta.

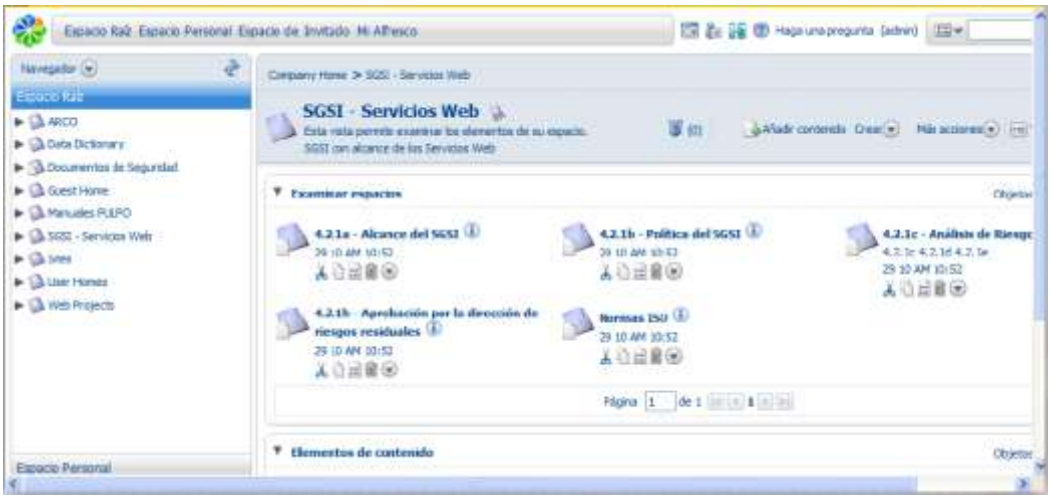


Figura 30: Gestión Documental (Espacio Raiz).

Fuente: Autor.

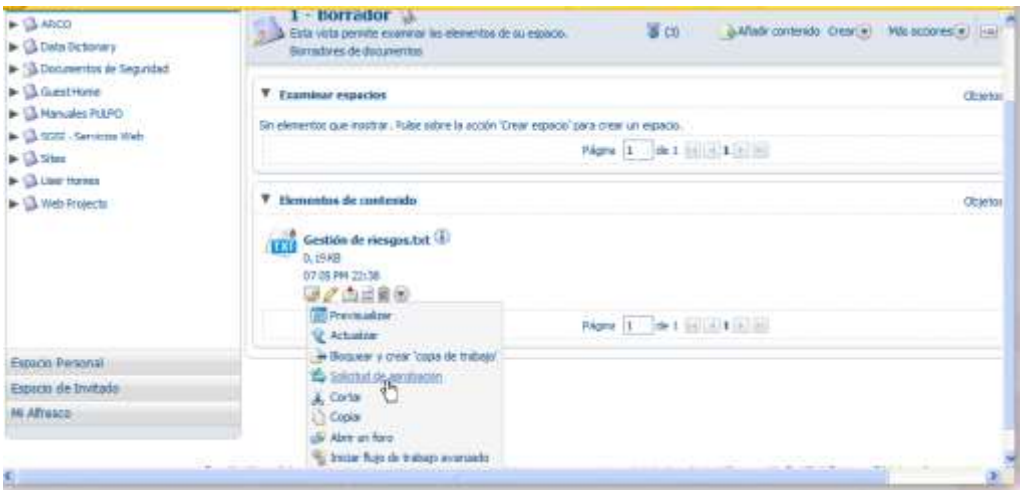


Figura 31: Aprobación y Difusión de documentos (ePulpo)

Fuente: Autor.

b) Gestión de activos.

Por medio de este componente se puede llegar a documentar y gestionar todos los activos dentro de la organización, de tal manera que se los pueda categorizar y sirva para realizar el análisis de riesgo.

Figura 32: Inventario de Activos (Panel Principal).

Fuente: Autor.

Figura 33: Inventario de Activos (Ingreso de Activos).

Fuente: Autor.

c) Gestión de Vulnerabilidades.

El componente de gestión de vulnerabilidades ayudará a gestionar todas las vulnerabilidades existentes en nuestros activos, este componente está subscrito a centros de investigación lo cual ayuda a que constantemente se esté actualizando con nuevas vulnerabilidades descubiertas.

Figura 34: Gestión de Vulnerabilidades (ePulpo).

Fuente: Autor.

d) Gestión de Riesgo.

La gestión de riesgo dentro de ePulpo permite añadir una capa de análisis y gestión, dentro del proceso de gestión de riesgos del activo se encuentra lo siguiente.

1. Ubicar el activo en una capa.
2. Ubicar un activo dentro de un grupo de activos.
3. Definir la clase de activo.
4. Definir la dependencia.

5. Definir la valoración en cada dimensión (disponibilidad, confidencialidad, integridad) del activo.
6. Visualizar el riesgo resultante.

A continuación se exponen las siguientes figuras, que muestran el proceso de gestión de riesgos.

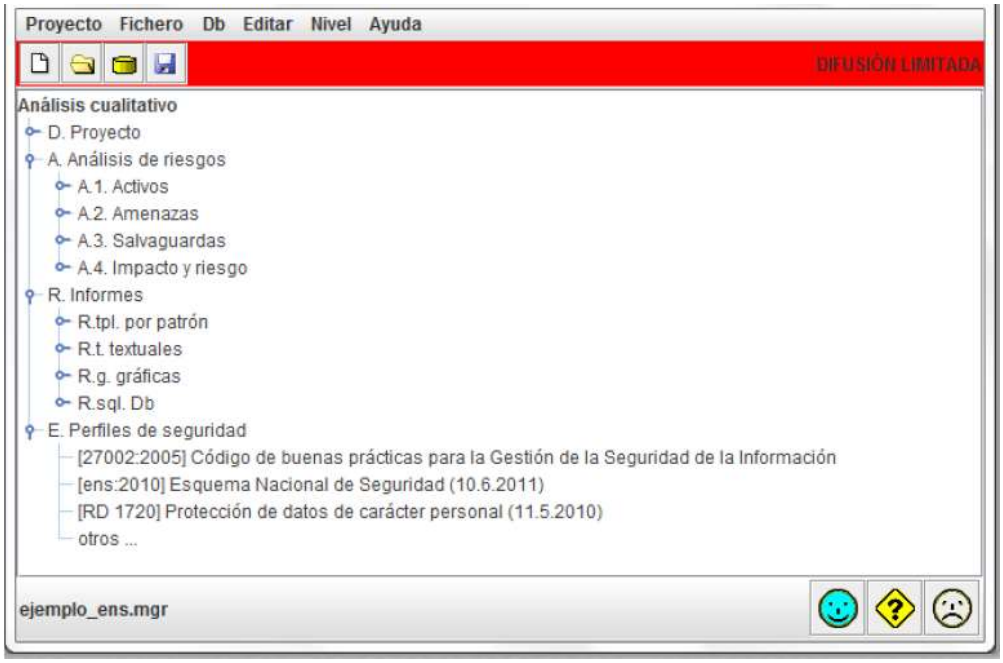


Figura 35: Análisis Cualitativo de activos.

Fuente: Autor.

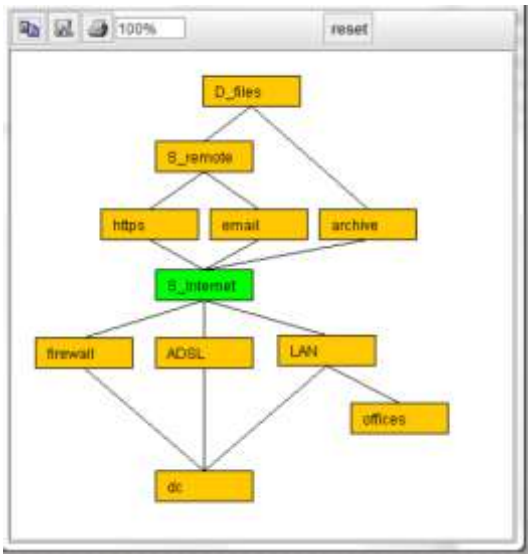


Figura 36: Dependencias entre activos (ePulpo).

Fuente: Autor.

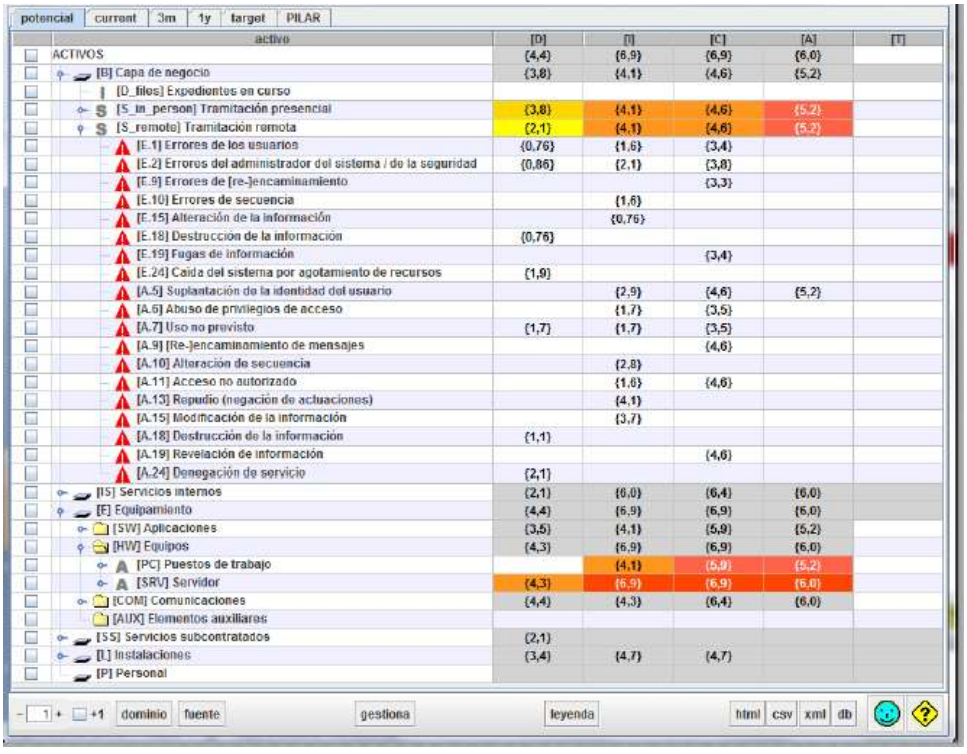


Figura 37: Riesgo Acumulado (ePulpo).

Fuente: Autor.

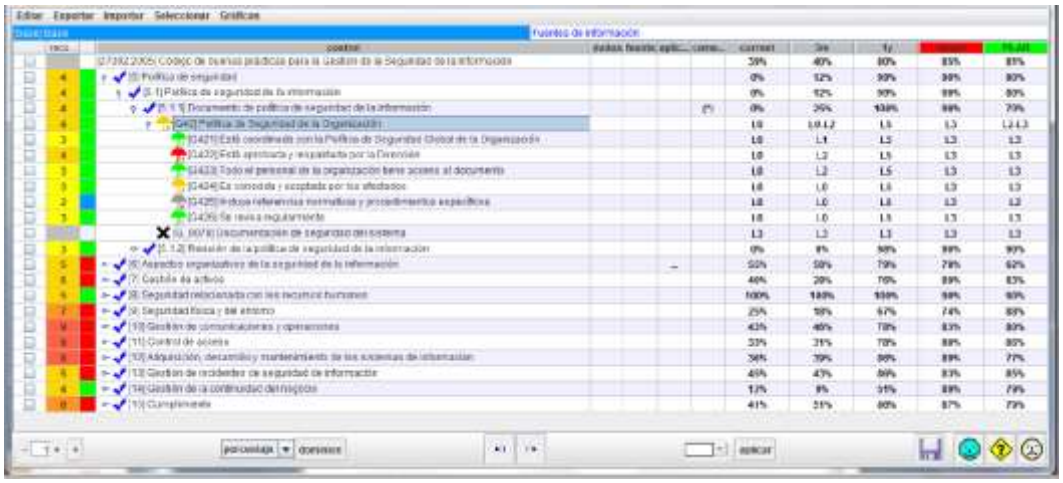
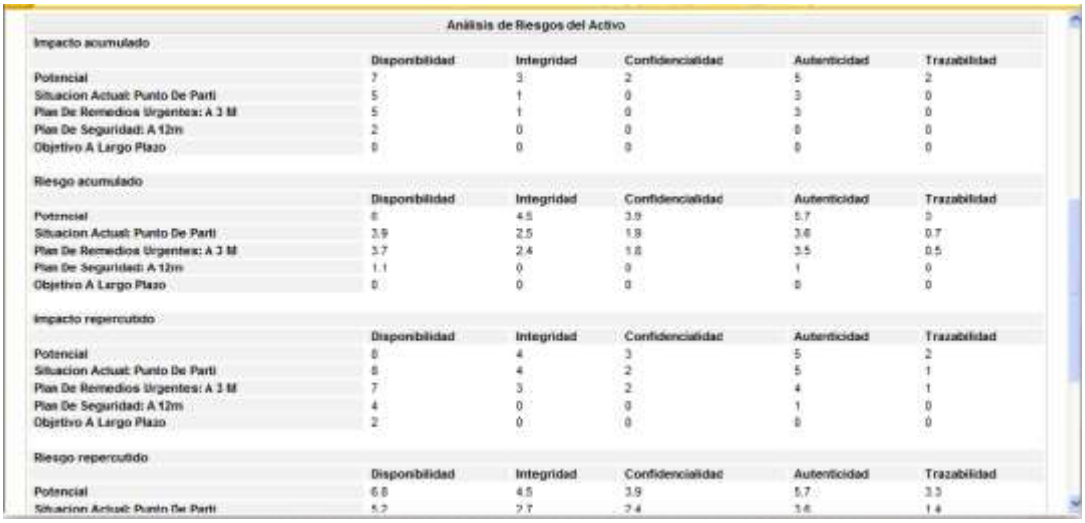


Figura 38: Análisis de Riesgos (ePulpo).

Fuente: Autor.



Análisis de Riesgos del Activo

Impacto acumulado

	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Potencial	7	3	2	5	2
Situacion Actual: Punto De Parti	5	1	0	3	0
Plan De Remedios Urgentes: A 3 M	5	1	0	3	0
Plan De Seguridad: A 12m	2	0	0	0	0
Objetivo A Largo Plazo	0	0	0	0	0

Riesgo acumulado

	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Potencial	6	4.5	3.9	5.7	3
Situacion Actual: Punto De Parti	3.9	2.5	1.9	3.6	0.7
Plan De Remedios Urgentes: A 3 M	3.7	2.4	1.8	3.5	0.5
Plan De Seguridad: A 12m	1.1	0	0	1	0
Objetivo A Largo Plazo	0	0	0	0	0

Impacto repercutido

	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Potencial	6	4	3	5	2
Situacion Actual: Punto De Parti	6	4	2	5	1
Plan De Remedios Urgentes: A 3 M	7	3	2	4	1
Plan De Seguridad: A 12m	4	0	0	1	0
Objetivo A Largo Plazo	2	0	0	0	0

Riesgo repercutido

	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Potencial	6.8	4.5	3.9	5.7	3.3
Situacion Actual: Punto De Parti	5.2	2.7	2.4	3.6	1.4

Figura 39: Resultado del análisis de riesgo (ePulpo).

Fuente: Autor.

Esta propuesta sigue el modelo expuesto por Deming "Planificar-Hacer-Verificar-Actuar", el cual se aplica para estructurar todos los procesos del Sistema de Gestión de Seguridad de la Información.

El modelo PHVA de Deming se incluye con el objetivo de aplicar el concepto de mejora continua, con el fin de lograr la eficacia del sistema por medio de la ejecución de acciones preventivas y correctivas, esto se lo debe de realizar en todos los aspectos involucrados en el Sistema de Gestión de la Seguridad de la Información, pues se indica, qué se debe mejorar la política de seguridad, los controles implementados, los planes de tratamiento de riesgos, entre otros. La descripción que expone la norma de la gestión se exhibe a continuación.

Acciones Correctivas.

Es la tarea que tiene la organización para solventar las posibles causas de las no conformidades que se han logrado evidenciar en el transcurso de la revisión y/o auditoría del Sistema de Gestión de la Seguridad de la Información, el principal objetivo de esta actividad es de prevenir la ocurrencia. Las organizaciones o entidades tienen el deber de documentar las acciones correctivas y de la misma manera según la normativa NTE INEN-ISO/IEC 27001:2011 se deben de definir los siguientes requisitos:

1) Identificar las no conformidades
2) Determinar las causas de las no conformidades
3) Evaluar la necesidad de acciones que aseguren que las no conformidades vuelven a ocurrir
4) Determinar e implementar la acción correctiva necesaria
5) Registrar los resultados de la acción tomada
6) Revisar la acción correctiva tomada

Acciones Preventivas.

En las organizaciones, esta acción tiene como objetivo mitigar las no conformidades que han sido detectadas de forma potencial y que afectan directamente o manera parcial al cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, previniendo su ocurrencia. Acorde a la normativa NTE INEN-ISO/IEC 27001:2011, los siguientes requisitos deben de encontrarse definidos en las acciones preventivas.

1) Identificar las no conformidades potenciales y sus causas
2) Evaluar la necesidad de acciones para impedir que las no conformidades ocurran
3) Determinar e implementar la acción preventiva necesaria
4) Registrar los resultados de la acción tomada
5) Revisar la acción preventiva tomada

En las acciones, debe de ser identificado los nuevos riesgos y los cambios que se ha realizado a los riesgos que ya se encuentren identificados, en relación a la evolución precipitada que en los últimos años ha tenido la tecnología de la información y las comunicaciones.

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones.

Una vez concluidos los estudios teóricos y prácticos de la presente investigación acerca del Análisis y diseño de un Sistema de Gestión de la Seguridad de la Información basado en el criterio de la norma NTE INEN-ISO/IEC 27001:2011 de un modelo de negocio aplicado en la comercialización y distribución de productos Químicos, es importante señalar los resultados más relevantes que se han encontrado en la misma en las siguientes conclusiones:

1. Al realizar un GAP análisis, se estará en la capacidad de formular un diagnóstico inicial de los niveles de seguridad que se tiene en la organización.
2. Al contar con un diagnóstico inicial de la seguridad de la información, se logrará plantear las metas que se requiere obtener en cuanto a la gestión de la seguridad de la información dentro de la organización.
3. Al desarrollar la metodología de diseño para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) empleando el criterio de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011, sobre los procesos de comercialización y distribución, se determinarán los mecanismos más idóneos para garantizar los principios de la confidencialidad, integridad y disponibilidad.
4. La presente propuesta puede ser utilizada como lineamiento de seguridad de la información, no únicamente para un modelo de negocio de comercialización y distribución de productos químicos.

5. Mediante el desarrollo adecuado del presente estudio de investigación, se puede llegar a planificar la siguiente etapa, que es la de implementación de un Sistema de Gestión de Seguridad de la Información.

6.2 Recomendaciones.

Se presentan las siguientes recomendaciones:

1. Para realizar la aplicación de este proyecto es necesario que se tenga los procesos de comercialización y distribución de productos químicos, correctamente levantados y documentados.
2. Es necesario que se tenga un departamento de seguridad de la información con sus respectivos responsables, de tal manera que se pueda distribuir la carga de trabajo que requiere para el análisis y diseño de un Sistema de Gestión de Seguridad de la Información.
3. Al aplicar este proyecto en un organización con un modelo de negocio de comercialización y distribución de productos químicos, es necesario se realice una revisión previa del presupuesto y carga operativa que este puede generar, ya que si no se lo realiza de manera correcta puede generar retrasos o pérdidas.
4. Para el mantenimiento del sistema de Gestión de Seguridad de la Información, se recomienda el uso de una herramienta o software, en la cual se pueda realizar un flujo de trabajo de tal manera que facilite la gestión del mismo.

LISTA DE REFERENCIAS

- (Español), C. E. (10 de Septiembre de 2010). *Comunidad ESET We Live Security (Español)*. Obtenido de Comunidad ESET We Live Security (Español): http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/
- *Comunidad ISO27001.es*. (2012). Obtenido de Comunidad ISO27001.es: http://www.iso27000.es/sgsi.html
- *Blog Metodologia02*. (Julio de 2013). Obtenido de Blog Metodologia02: http://metodologia02.blogspot.com/p/operacionalizacion-de-variables.html
- *Blog tiposdeinvestigacion*. (4 de febrero de 2013). Obtenido de Blog tiposdeinvestigacion: http://www.tiposdeinvestigacion.com/
- *Comunidad ISO TOOLS EXCELLENCE* . (29 de Mayo de 2013). Obtenido de Comunidad ISO TOOLS EXCELLENCE : http://www.nytimes.com/2009/09/13/us/13water.html?em
- Agustín López Neira. (2012). *Comunidad ISO27001.es*. Obtenido de Comunidad ISO27001.es: http://www.iso27000.es/sgsi.html
- Alegsa, L. (2010). *ALEGSA*. Obtenido de ALEGSA: http://www.alegsa.com.ar/Dic/seguridad%20informatica.php
- Avellaneda, J. C. (12 de Junio de 2014). *Blog sgsi-iso27001*. Obtenido de Blog sgsi-iso27001: http://sgsi-iso27001.blogspot.com/
- Bortnik , S. (16 de Abril de 2010). *ESET We Live Security*. Obtenido de ESET We Live Security: http://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/

- CERT. (2013). *Centro de Respuestas a Incidentes de Seguridad Informática del Uruguay* . Obtenido de Centro de Respuestas a Incidentes de Seguridad Informática del Uruguay : www.cert.uy
- Diccionario de la Lengua Española. (2010). *Diccionario de la Lengua Española.* Madrid.
- Federico Pacheco. (10 de Septiembre de 2010). *We Live Security*. Obtenido de We Live Security: http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/
- Federico Pacheco. (10 de Septiembre de 2010). *We Live Security*. Obtenido de We Live Security: http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/
- García, A., & Alegre, M. (2011). *Seguridad Informática.* S.A. EDICIONES PARANINFO.
- Hidalgo, I. V. (20 de Mayo de 2012). *Blog GestioPolis*. Obtenido de Blog GestioPolis: http://www.gestiopolis.com/canales5/eco/tiposestu.htm
- INSEMONT, C. (3 de Octubre de 2012). *Comunidad INSEMONT*. Obtenido de Comunidad INSEMONT: http://www.insemot.eu/es/gesti%C3%B3n-de-un-si/216-what-is-an%C2%A0information-security-management-system-isms
- Institute, P. M. (2013). *Guía de los fundamentos para la dirección de proyectos (guía del PMBOK®) -- Quinta edición.* Project Management Institute.
- Instituto Ecuatoriano de Normalización. (2010). *Norma Técnica Ecuatoriana NTE-ISO/IEC 27001:2011. Primera Edición.* Quito.

- ISACA. (2011). *Manual de preparación para el examen CISM.* Guayaquil: ISACA.
- Jacques M. Chevalie. (2009). *SAS." Guía para la Investigación Colaborativa y la Movilización Social.* Madrid: Plaza y Valdes.
- Lemus, R. G. (2014). Seguridad de la Información. *Revista de la segunda Cohorte del Doctorado en Seguridad Estratégica*, 373.
- Ministerio de Hacienda y Administraciones Públicas de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Madrid.
- NICCS. (2015). *National Security for Cybersecurity Carrers and Studies*. Obtenido de National Security for Cybersecurity Carrers and Studies: niccs.us-cert.gov/careers/careers-home
- Normalización, I. d. (2010). *Norma ISO 27035* .
- Normalización., I. E. (2010). *Norma Técnica Ecuatoriana NTE-ISO/IEC 27001:2011. Primera Edición.* Quito.
- Ochoa Ovalles S. y Cervantes Sánchez, O. (Julio de 2012). *EUMED*. Obtenido de EUMED: http://www.eumed.net/rev/cccss/21/oocs.html
- PMG-SSI, C. (20 de Enero de 2014). *Comunidad PMG-SSI*. Obtenido de Comunidad PMG-SSI: http://www.pmg-ssi.com/2014/01/que-es-un-sgsi/
- Ponemon Institute. (October 2012.). *2012 Cost of Cyber Crime Study: United States.* Unites States of America: Ponemon Institute.
- Ramóm Robles y Alvaro Rodriguez De Roa. (Junio de 2006). *Asociacion Española de la Calidad*. Obtenido de Asociacion Española de la Calidad: http://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

- Robles, R., & Rodriguez De Roa, A. (Junio de 2006). *Asociacion Española de la Calidad*. Obtenido de Asociacion Española de la Calidad: http://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128
- The Deming Bio. (2010). *Deming Collaboration*. Obtenido de Deming Collaboration: http://demingcollaboration.com/language/spanish/biografia-completa-de-deming/
- Winter Park Public Library. (18 de Agosto de 2001). *Winter Park Public Library*. Obtenido de Winter Park Public Library: http://www.wppl.org/wphistory/PhilipCrosby/index.html

ANEXO 1: ANÁLISIS DE BRECHAS (GAP ANÁLISIS).

Tabla 29: Plantilla estándar para la realización del análisis de brechas.

OK.	Estado que evidencia de que la revisión ha pasado exitosamente.
OM (Oportunidad de Mejora).	Estado que evidencia que la revisión ha pasado con observaciones.
NC (No Conformidad).	Estado que evidencia que la revisión no ha pasado la revisión.

Requerimiento / Elementos	**Cumplimiento (OK/OM/NC)**	**Observaciones/Evidencias.**
4.1 Requisitos Generales La organización debe crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI documentando dentro del contexto de las actividades empresariales generales de la organización y de los riesgos que esta afronta. A efectos de esta norma, el proceso utilizado se basa en el modelo PCDA.		
4.2.1 Creación del SGSI.		

Requerimiento / Elementos	**Cumplimiento (OK/OM/NC)**	**Observaciones/Evidencias.**
4.2.1a) Definir el alcance y los límites del SGSI en términos de las características de la actividad empresarial, de la organización, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier excusa del alcance.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.1b) Definir una política del SGSI acorde con las características de la actividad empresarial, la organización, su ubicación, sus activos y tecnología que; 1) Incluya un marco para la fijación de objetivos y establezca una orientación general sobre las directrices y principios de actuación en relación con la seguridad de información. 2) Tenga en cuenta los requisitos de la actividad empresarial, los requisitos legales o reglamentarios y la orientación de seguridad contractuales. 3) Este alineada con el contexto de la estrategia de gestión de riesgos de la organización contexto en el que tendrá lugar la creación y mantenimiento el SGSI 4) Establezca criterios estimados de riesgo (4.2.1c) 5) Sea aprobada por la dirección.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.1c) Definir el enfoque de la evaluación de riesgos de la organización. 1. Especificar una metodología de evaluación de riesgos adecuada para el SGSI, las necesidades de negocio identificadas en materia de seguridad de la información de la empresa y los requisitos legales y reglamentarios. 2. Desarrollar criterios de aceptación de riesgo y fijar los niveles de riesgo aceptable.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.1d) Identificar los riesgos. 1. Identificar los activos que están dentro del ámbito de aplicación del SGSI y a los propietarios de estos activos. 2. Identificar las amenazas a que están expuestos esos activos. 3. Identificar las vulnerabilidades bajo las que podrían actuar dichas amenazas 4. Identificar los impactos que sobre los activos puede tener una pérdida de confidencialidad, integridad y disponibilidad en los mismos.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.1e) Analizar y valorar los riesgos 1. Evaluar los efectos en la actividad empresarial de la organización que pudieran derivarse de eventuales fallos de seguridad, teniendo en cuenta las consecuencias de una perdida de confidencialidad, integridad de los activos. 2. Evaluar la probabilidad, de una forma realista, de que se produzcan fallos de seguridad a la luz de la amenazas y vulnerabilidades existentes, los impactos asociados a los activos y los controles de implementación 3. Estimar los niveles de riesgo 4. Determinar si los riesgos son aceptables o si requieren un tratamiento conforme a los criterios de aceptación de riesgo establecidos en 4.2.1c).		

Requerimiento / Elementos	**Cumplimiento (OK/OM/NC)**	**Observaciones/Evidencias.**
4.2.1f) Identificar y evaluar las opciones para el tratamiento de riesgos Las posibles acciones a realizar, entre otras, son las siguientes: 1. Aplicar los controles adecuados 2. Asumir los riesgos de manera consciente y objetiva, conforme a las políticas de la organización y a los criterios de aceptación de riesgo. 3. Evitar los riesgos 4. Transferir los riesgos asociados a la actividad empresarial a otras partes, como por ejemplo compañías de seguros o proveedores		
4.2.1g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.		
4.2.1h) Obtener la aprobación, por parte de la Dirección, de los riesgos residuales propuestos.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.1i) Obtener la autorización de la Dirección para implementar y operar el SGSI.		
4.2.1j) Elaborar una declaración de aplicabilidad. Una declaración de aplicabilidad debe incluir lo siguiente: 4. Los objetivos de control y los controles seleccionados en 4.2.1g) y las justificaciones de su selección; 5. Los objetivos de control y los controles actualmente implementados (4.2.1e). 6. La exclusión de cualquier objetivo de control y control del anexo A y la justificación de esta exclusión.		
4.2 Implementación y Operación del SGSI		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.2a) Formular un plan de tratamiento de riesgos que identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuados para gestionar los riesgos de la seguridad de la información (véase 5).		
4.2.2b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que tengan en cuenta la financiación y la asignación de funciones y responsabilidades.		
4.2.2c) Implementar los controles seleccionados en **4.2.1g** para cumplir los objetivos de control.		
4.2.2d) Definir el modo de medir la eficacia de los controles o de los grupos de controles seleccionados y especificar como tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir unos resultados comparables y reproducibles (Véase 4.2.3c)		

Requerimiento / Elementos	**Cumplimiento (OK/OM/NC)**	**Observaciones/Evidencias.**
4.2.2e) Implementar programas de formación y concienciación (Véase 5.2.2).		
4.2.2f) Gestionar la Operación del SGSI.		
4.2.2g) Gestionar los recursos del SGSI.		
4.2.2h) Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad (Véase 4.2.3a)		
4.2.3 Supervisión y Revisión del SGSI		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.3a) Ejecutar procedimientos de supervisión y revisión, así como otros mecanismos del control para: 1. Detectar lo antes posible los errores en los resultados de lo procesado. 2. Identificar lo antes posible las debilidades del sistema de seguridad así como el aprovechamiento de éstas tanto con o sin éxito, y los incidentes 3. Permitir a la Dirección determinar si las actividades de seguridad delegadas en otras personas o llevadas por medios informáticos o a través de tecnologías de la información, dan los resultados esperados 4. Ayudar a detectar eventos de seguridad y por tanto a prevenir incidentes de seguridad mediante el uso de indicadores		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.3b) Realizar revisiones periódicas de la eficacia del SGSI teniendo en cuenta los resultados de las auditorias de seguridad, los incidentes, los resultados de las mediciones de la eficacia, las sugerencias asi como los comentarios de todas las partes interesadas. Estas revisiones incluyen el cumplimiento de la política, y de los objetivos del SGSI, y la revisión de los controles de seguridad.		
4.2.3c) Medir la eficacia de los controles para verificar si se han cumplido los requisitos de seguridad.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.3d) Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles de riesgo aceptables que han sido identificados, teniendo en cuenta los cambios en: 1. La Organización 2. La Tecnología 3. Los objetivos y requisitos empresariales 4. Las amenazas identificadas 5. La eficacia de los controles implementados 6. Los factores externos, como por ejemplo los cambios del entorno legal o reglamentario, de las obligaciones contractuales y del clima social.		
4.2.3e) Realizar las auditorías internas del SGSI en intervalos planificados (Véase 6). Nota: Las auditorías internas, a veces se denominan auditorias por primera parte, las lleva a cabo la propia organización.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.3f) Realizar por parte de la Dirección una revisión del SGSI, con carácter regular para asegurar que el ámbito de aplicación sigue siendo adecuado y que se identifican mejoras del proceso del SGSI (Véase 7.1)		
4.2.3g) Actualizar los planes de seguridad teniendo en cuenta las conclusiones de las actividades de supervisión y revisión.		
4.2.3h) Registrar las acciones e incidencias que pudieran afectar a la eficacia o al funcionamiento del SGSI (Véase 4.3.3)		
4.2.4 Mantenimiento y mejora del SGSI		
4.2.4a) Implementar en el SGSI las mejoras identificadas		
4.2.4b) Aplicar las medidas correctivas y preventivas adecuadas de acuerdo con los apartados 8.2 y 8.3, sobre la base de la experiencia en materia de seguridad de la propia organización y de otras organizaciones.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.2.4c) Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle acorde con las circunstancias.		
4.2.4d) Asegurar que las mejoras alcances los objetos previstos.		
4.3 Requisitos de la Documentación		
4.3.1a) Declaración documentada de la política.		
4.3.1b) El alcance del SGSI		
4.3.1c) Los procedimientos y mecanismos de control que soportan al SGSI.		
4.3.1d) Una descripción de la metodología de evaluación de riesgo.		
4.3.1e) El informe de evaluación de riesgos		
4.3.1f) El plan de tratamiento de riesgos.		
4.3.1g) Los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles		

Requerimiento / Elementos	**Cumplimiento (OK/OM/NC)**	**Observaciones/Evidencias.**
4.3.1h) Los registros requeridos por esta norma (4.3.3)		
4.3.1i) La declaración de aplicabilidad		
4.3.2 Control de Documentos		
4.3.2a) Aprobar el formato de los documentos previamente a su distribución.		
4.3.2b) Revisar, actualizar y volver a aprobar los documentos, según vaya siendo necesario.		
4.3.2c) Asegurar que están identificados los cambios, así como el estado del documento que contiene la última revisión.		
4.3.2d) Asegurar que las versiones correspondientes de los documentos estén disponibles.		
4.3.2e) Asegurar que los documentos aparezcan legibles y fácilmente identificables.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
4.3.2f) Asegurar que los documentos estén disponibles para todo el que lo necesita, y se transfieren, almacenan y destruyen de acuerdo con los procedimientos aplicables a su clasificación.		
4.3.2g) Asegurar que los documentos procedentes del exterior estén identificados		
4.3.2h) Asegurar que la distribución de los documentos sea controlada		
4.3.2I) Prevenir el uso no intencionado de documentos obsoletos		
4.3.2j) Aplicar una identificación adecuada a los documentos obsoletos que son retenidos con algún propósito.		
4.3.3 Control de Registros		
4.3.3 Se debe de crear y mantener registros para proporcionar evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.		
5. Responsabilidades de la dirección.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
5.1 Compromiso de la Dirección. La dirección debe suministrar evidencias de su compromiso para crear, implementar, operar, superar, revisar, mantener y mejorar el SGSI.		
5.2 Gestión de los Recursos.		
5.2.1 Provisión de los Recursos. La organización debe determinar y proporcionar los recursos necesarios.		
5.2.2 Concienciación, formación y capacitación. La organización debe de asegurarse de que todo el personal al que se hayan asignado responsabilidades definidas en el SGSI sea competente para llevar a cabo las tareas requeridas.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
6. Auditorías Internas del SGSI Determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI. a) Cumplen los requisitos de esta norma, así como la legislación y normativas aplicables b) Cumplen los requisitos de seguridad de la información identificados. c) Se implantan y mantienen de forma efectiva. d)Dan el resultado esperado		
7. Revisión del SGSI por la Dirección. Revisión por la dirección por lo menos una vez al año, para asegurar que se mantiene su conveniencia, adecuación y eficacia.		
8. Mejora del SGSI.		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
8.1 Mejora Continua. La organización debe mejorar de manera continua la eficacia del SGSI, mediante el uso de la política y de los objetos de seguridad de la información, de los resultados de las auditorias, del análisis de la monitorización de eventos, de las acciones correctivas y preventivas y de las revisiones de dirección (Véase 7).		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
8.2 Acciones Correctivas El procedimiento documentado para las acciones correctivas debe definir los requisitos para: a) Identificar las no conformidades b) Determinar las causas de las no conformidades c) Evaluar la necesidad de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse. d) Determinar implantar las acciones de las correctivas necesarias e) Registrar los resultados de las acciones realizadas f) Revisar las acciones correctivas realizadas		

Requerimiento / Elementos	Cumplimiento (OK/OM/NC)	Observaciones/Evidencias.
8.3 Acciones Preventivas Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas potenciales. a) Identificar las posibles no conformidades y sus causas. b) Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades. c) Determinar e implementar las acciones preventivas necesarias. d) Registrar los resultados de las acciones adoptadas e) Revisar las acciones preventivas adoptadas.		

Fuente: (Instituto Ecuatoriano de Normalización, 2010)**.**

Elaborado por: Autor.

ANEXO 2: MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Manual de Gestión de Seguridad de la Información de una industria Química.		
Sistema de Gestión de Seguridad de la Información.		
CODIGO. **EC-155**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

“Manual de Seguridad de la Información de una Industria Química.”

ENERO DEL 2015.

Manual de Gestión de Seguridad de la Información de una industria Química.		
Sistema de Gestión de Seguridad de la Información.		
CODIGO. EC-155	ELABORADO. 20/01/2015	Versión. 01

Tabla de Contenido.

1. Objetivo.

Este documento describe los aspectos más relevantes del Sistema de Gestión de Seguridad de la Información de una industria química, con el fin de asegurar una base común para el desarrollo de estándares de seguridad de la información en la organización y la práctica efectiva en la administración de la misma, según sus necesidades y objetivos, para cumplir los requisitos de gestión de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011 y como parte complementaria del proceso de Gestión de la Información.

2. Alcance y Exclusiones.

2.1 Alcance y Limites del SGSI.

El alcance del SGSI de la industria química corresponde a:

"SERVICIOS DE COMERCIALIZACIÓN Y DISTRIBUCIÓN DE PRODUCTOS QUIMICOS"

Sobre los procesos mencionados anteriormente se van a aplicar todas las políticas, procedimientos y controles necesarios para lograr una gestión de la seguridad de la información de manera óptima y eficiente.

3. Glosario.

Activo de Información.

Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización. Ej.: bases de datos, archivos, programas, manuales, equipos de comunicación, la imagen de la empresa. La información como activo corporativo, puede existir de muchas formas: Impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en video, suministrada en una conversación, conocimiento de las personas.

Bases de Datos.

Herramienta especial de investigación que permite la búsqueda y localización de información de carácter técnico.

Confidencialidad.

Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados. (Instituto Ecuatoriano de Normalización, 2010)

Conformidad.

Cumplimiento de un requisito.

Disponibilidad.

Propiedad de la que la información, sea accesible y utilizable por solicitud de una entidad autorizada. (Instituto Ecuatoriano de Normalización, 2010)

Integridad.

Propiedad de salvaguardar la exactitud y estado completo de los activos. (Instituto Ecuatoriano de Normalización, 2010)

Manual de Gestión.

Documento que especifica el sistema de gestión de una organización.

Normas Técnicas.

Establecen las características o especificaciones de un producto, servicio o procesos.

Proceso.

Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y transforman elementos de entrada en resultados.

Seguridad de la Información.

Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Instituto Ecuatoriano de Normalización, 2010)

S.G.S.I.

Sistema de Gestión de Seguridad de la Información.

4. Introducción al Sistema de Gestión de Seguridad de la Información.

4.1 Gestión por procesos.

El Sistema de Gestión de la industria química.; es representada por medio del Mapa de Procesos que ha sido definido bajo el modelo de gestión planteado por la norma NTE – ISO 9001:2000; con el que se garantiza la confiabilidad y la competitividad de los servicios y productos a entregar al cliente.

4.2 Planificación del Sistema de Gestión de Seguridad de la Información.

El Sistema de Gestión avala la adecuada implementación, gestión y operación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información en cualquier organización.

Principios del SGSI.

- **Confidencialidad:** La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados (Instituto Ecuatoriano de Normalización, 2010).
- **Integridad:** La propiedad de salvaguardar la exactitud y complejidad de los activos (Instituto Ecuatoriano de Normalización, 2010).

- **Disponibilidad:** La propiedad de ser accedida y utilizable por una entidad autorizada (Instituto Ecuatoriano de Normalización, 2010).

Documentos del Sistema.

Este manual como cualquier otro documento sigue el Procedimiento del Control de Documentos para su elaboración, revisión, publicación y distribución.

La estructura jerárquica de la documentación es la siguiente.

- Manual de Gestión de Seguridad de la Información.
- Procedimientos.
- Control de documentos.
- Revisión por la dirección.
- Análisis y Evaluación de riesgos.
- Acciones Correctivas y preventivas.
- Instructivo para auditorías internas.

Todos los documentos relacionados con el Sistema de Gestión de Seguridad de la Información, se encuentran relacionados en el listado maestro de documentos.

5. Responsabilidad de la dirección.

5.1 Políticas y Objetivos de Seguridad de la Información.

En el Sistema de Gestión de Seguridad de la información, se ha definido una política de seguridad de la información el cual se expone a continuación.

Gestionar la seguridad de la información de nuestros clientes los cuales contratan nuestros servicios para la comercialización y distribución de productos químicos, bajo los lineamientos corporativos de Seguridad de la información, asegurando de esta forma el cumplimiento de las características de confidencialidad, integridad y disponibilidad, los requisitos de la empresa y la normativa interna y legislativa que sea aplicable. Así mismo, gestionar las metodologías y herramientas que permiten minimizar los riesgos en los activos de información tanto críticos como no críticos, teniendo en cuenta criterios de evaluación de riesgos.

Para el SGSI de la industria química en alineación con el cumplimiento de la política y directrices de seguridad de información, se plantean los siguientes objetivos:

- Garantizar que los riesgos de la seguridad de la información, asociados a los activos de información, sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistematizada, estructurada,

repetible, eficiente y adaptada a los cambios que se reproduzcan en los riesgos, el entorno y las tecnologías.

- Mantener los riesgos identificados, en un nivel de exposición de riesgo siempre menor al nivel que la industria química ha decidido asumir.
- Mantener durante todo el ciclo de operación de la industria química, la confidencialidad definida por los usuarios, mediante la implementación de controles y mecanismos de manejo de la información acorde con el análisis de riesgos.
- Mejorar continuamente los comportamientos seguros, con el fin de minimizar las vulnerabilidades, logrando así, un entorno más seguro en las actividades laborables y en general los procesos desarrollados.
- Velar por el cumplimiento de la Legislación Nacional.
- Proteger los recursos de información de la industria química y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el
- Cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

Las Directrices de Seguridad de la Información son la declaración de las responsabilidades de conducta que deberán de ser cumplidas por los destinatarios de la Política en el Tratamiento de la Información propia o de terceros, que a su vez se constituye en un derecho y en una garantía para sus propietarios.

Las Directrices se encuentran organizadas de acuerdo con los apartados de la norma establecidos por el estándar de la Seguridad de la Información NTE ISO/IEC 27001:2011, base para el desarrollo de la política.

Directriz 1. Política de Seguridad de la Información.

a) La Política junto con su Sistema de Gestión de Seguridad de la Información debe ser desarrollada y actualizada acorde con los riesgos, los requerimientos institucionales y las leyes locales de los países en los cuales la industria química tenga operación.

Cada año cuando la industria química lo considere necesario, revisará la vigencia de la política y su concordancia con el Sistema de Gestión de Seguridad de la Información atendiendo a los riesgos identificados, la normativa legal que de tiempo en tiempo resulte aplicable, las nuevas necesidades y situaciones de la entidad y las mejores prácticas como parte de la gestión normal de la industria química.

Directriz 2. Organización de la Seguridad de la Información.

a) **La organización de la Seguridad de la Información debe establecerse y mantenerse acorde con las necesidades de la entidad y las mejores prácticas, con el fin de implantar y gestionar el proceso de Seguridad de la Información.**

b) **Los terceros que efectúen el tratamiento de información propia de la industria química o sobre la cual la entidad sea responsable, deberá cumplir con la política junto con su sistema de Gestión de Seguridad de la Información.**

Cada rol debe identificar, analizar, evaluar, tratar y monitorear el cumplimiento dela política, con una base de comunicación y creación de una verdadera cultura de Seguridad de la Información en la entidad.

El uso de los recursos de información en la organización por personal que no pertenece a la entidad ya sea local o remotamente, debe ser formalizada por medio de acuerdos de confidencialidad que hagan obligatorio el cumplimiento de la presente política.

Directriz 3. Gestión de Activos de Información.

a) **Cada activo de información de la organización debe tener asignado un responsable, quien debe clasificarlo, basado en la sensibilidad, valor, riesgo de pérdida o compromiso del mismo y/o requerimientos legales.**

b) **La Información de la organización es un activo estratégico, por lo tanto debe ser protegido permanentemente.**

c) **Los recursos de información son provistos a los usuarios para uso exclusivo y excluyentemente de los fines con los cuales le fue entregada y/o permitido su acceso por parte del responsable.**

d) **La organización realiza el tratamiento de la información de terceros sobre la cual es responsable, con el mismo grado de diligencia con que realiza el tratamiento de su propia información.**

La información que la industria química utilice para el desarrollo de sus objetivos tiene asignado un responsable, quien la utiliza y es el que responde por su correcto tratamiento. Así, él toma las decisiones que son requeridas para la protección de su información y determina quienes son los usuarios y sus privilegios de tratamiento. Cada responsable debe conocer la

información que debe cuidar, vigilar su correcto tratamiento, los lugares donde reside y los usuarios de la misma.

Los niveles de clasificación de la información se deben realizar con base en su sensibilidad, valor, riesgo de pérdida o compromiso, y/o requerimientos legales de retención. Dichos niveles serán divulgados y oficializados a los usuarios de la información para asegurar que los niveles de protección son entendidos y se mantienen a través de la entidad.

Cada nivel de clasificación tendrá un conjunto de controles determinados por la industria química. Dichos controles serán diseñados para proveer un nivel de protección de la información apropiado y consistente dentro de la entidad, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Directriz 4. Seguridad de los Recursos Humanos.

a) **La organización establecerá un programa permanente de capacitación y transformación de la cultura en Seguridad de la Información.**
b) **La organización proveerá los mecanismos necesarios que le permitan a los usuarios cumplir con sus responsabilidades en**

Seguridad de la Información desde su vínculo inicial hasta que cesen sus compromisos con la entidad.

Manual de Gestión de Seguridad de la Información de una industria Química.		
Sistema de Gestión de Seguridad de la Información.		
CODIGO. **EC-155**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

La industria química debe contar con un programa permanente de creación de cultura de la Seguridad de la Información con medidas de protección y/o controles, que permitan asegurar que los destinatarios de la política conozcan y entiendan sus responsabilidades en Seguridad de la Información, así como sobre las continuas amenazas que ponen en riesgo la información que manejan. La organización debe contar con mecanismos de difusión para que los destinatarios de la política se sensibilicen acerca de los procedimientos de Seguridad de la Información que deben aplicar en la realización de sus funciones.

En los procesos de selección, reclutamiento, incorporación, estadía y cierre de contrato de funcionarios de la industria química, deberá pasar por un proceso de selección con la investigación adecuada, con el fin de mitigar los riesgos en el tratamiento de la información de la organización. Los criterios para definir el nivel de investigación serán establecidos por la Vicepresidencia de Talento Humano.

Directriz 5. Seguridad Física y del Entorno.

a) **Cada área física de la organización debe de tener un nivel de seguridad acorde con el valor y la sensibilidad de la información que se procesa y administra en ellas.**

La seguridad física de la organización debe de basarse en una definición de permisos y áreas declaradas como seguras, las cuales serán

protegidas por medio de controles apropiados. Estos deben ser consistentes con el valor y la sensibilidad de la información que contienen los derechos mínimos de acceso a las áreas los cuales deben ser otorgados teniendo en cuenta si los sitios de trabajo son permanentes o no.

Los recursos de información de la organización y los equipos de procesamiento donde residan deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos de información, intencional o no intencional, para evitar la interrupción de las actividades de la entidad.

Directriz 6. Gestión de Comunicación y Operaciones.

a) **La organización debe de preservar el nivel de protección de la información cuando pasa a través de redes diferentes a la red privada de la entidad.**

La realización de un cambio tecnológico que no considere los requerimientos de Seguridad de la Información hace que la organización esté

expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la política y sus respectivos estándares, y en caso de exponer a la entidad a un riesgo en seguridad de la información, este debe ser identificado, evaluado, documentado, reportado, asumido y administrado por el respectivo responsable de la información.

La organización debe contar con un programa de seguridad que evite el ingreso de código no autorizado, estableciendo unidades de reacción inmediata y los medios de difusión que mitiguen el impacto en caso de ser detectado un evento. Como un medio de mitigación se debe contar con un proceso de copia y recuperación de la información que permita tener copias acorde con los niveles de servicios comprometidos y el riesgo de ingreso de código no autorizado. El tratamiento de dichas copias debe incluir mecanismos que preserven la confidencialidad e integridad de la información crítica.

Las conexiones desde y hacia la red privada de la organización, deben de realizarse de una manera segura para preservar la integridad, confidencialidad y disponibilidad. El flujo de información desde redes no confiables debe realizarse desde los puntos autorizados por la entidad.

Directriz 7. Control de Acceso.

a) **Cada usuario que accede a la información de la organización debe disponer de un medio de identificación y su acceso debe ser controlado a través de una autenticación personal.**
b) **El tratamiento de la información de la organización debe ser dado, mantenido y controlado con base en una necesidad de negocio demostrada.**

Cada usuario es responsable por sus acciones mientras utiliza cualquier recurso de información de la organización. Por lo tanto, la identidad de cada usuario de los recursos de información deberá ser establecida y autenticada de una manera única. Esta identidad de ninguna manera o por ninguna circunstancia podrá ser compartida.

Los niveles de acceso deben ser revisados periódicamente por el respectivo responsable de la información y cualquier desviación será tratada como un incidente en seguridad de la información.

Directriz 8. Adquisición, desarrollo y mantenimiento de Sistemas de Información.

a) **Cada solución que se implemente en la organización debe incluir los requerimientos mínimos de Seguridad de la Información, durante su ciclo de vida.**

Los responsables por la provisión de soluciones deben de crear y mantener una metodología que controle el ciclo completo de adquisición, desarrollo y mantenimiento seguro de las soluciones de información e infraestructura. Los requerimientos de seguridad de la información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura. De ser necesario el desarrollo interno, los requerimientos deben ser incluidos dentro de los sistemas y si una modificación es solicitada, debe cumplir estrictamente con los requerimientos de Seguridad de la

Información que han sido previamente establecidos. La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como para desarrollo de soluciones.

Cada solución de información o de infraestructura debe mantener durante su ciclo de vida, una gestión de riesgo que informe permanentemente el nivel de exposición que representa para la organización.

Directriz 9. Gestión de Incidentes de la Seguridad de la Información.

a) **La organización vigilará permanentemente el cumplimiento de la Política de Seguridad de la Información y cuando exista una violación será alertará en el mismo instante a las instancias oficiales establecidas para tal fin.**

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas a las áreas responsables por su tratamiento de manera inmediata (alertas). Se debe desarrollar un programa de tratamiento de incidentes de seguridad de la información que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información de la organización. Dicho programa debe incluir la definición de una organización de reacción inmediata, con el objetivo de atender estas y otras situaciones que la entidad considere como críticas

El responsable de la información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata a la entidad de reacción inmediata. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

Directriz 10. Gestión de continuidad del negocio.

a) **Los recursos de Información y los procesos definidos por la organización, deben contar con un Plan de Continuidad de**

Negocio soportados por una organización propia y estar preparados ante fallas mayores y/o desastres.

Los procesos críticos establecidos por la industria química deben garantizar que sus activos de información estén disponibles para su tratamiento autorizado cuando la entidad lo requiera en la ejecución de sus tareas regulares. Por lo que una organización definida por el responsable del proceso, debe diseñar, documentar, implementar, entrenar, divulgar y probar, mantener y medir periódicamente procedimientos para asegurar una recuperación de la operación en el tiempo requerido, sin disminuir los niveles de seguridad de la información establecidos.

Estos planes deben ser independientes tanto del medio tecnológico que utilice la organización, como de la posibilidad de que la información se dañe, se destruya o no este disponible por un periodo de tiempo. Cada plan debe ser clasificado y manejado acorde con los niveles de la información objeto de la recuperación.

Directriz 11. Cumplimiento.

a) **La organización vigilará permanentemente el cumplimiento de las Políticas de Seguridad de la Información cuando exista una violación debe ser detectada e informada a las instancias oficiales establecidas para tal fin.**

b) La organización debe cumplir con las leyes y regulaciones de Seguridad y Privacidad de la Información de los países donde opere.

Las situaciones o acciones que violen la presente política deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Se entenderán incluidas a la política las regulaciones nacionales e internacionales que de tiempo en tiempo se expidieren y que se relacionen con la misma. Cuando de la aplicación de tales normas se presentare un conflicto, se entenderá que aplica la más restrictiva, es decir, aquella que exija el mayor grado de seguridad.

Así mismo y con el fin de mantener un nivel de seguridad en line con el negocio de la organización, esta política se debe de apoyar en las mejores prácticas de la seguridad de la información y aquellos que el mercado y la entidad reconozcan como tal.

5.2 Liderazgo y Compromiso.

Todas las actuaciones del Equipo de Dirección de la industria química, el cual se encuentra formado por el Director, Jefe de Unidad y Líder de la organización, así como todos los colaboradores de la organización, están enmarcadas en las disposiciones del Código de Ética de la organización.

El Código de Buen Gobierno estructura y compila las políticas, normas y sistemas para preservar, mantener y promulgar la integridad ética empresarial y divulgar al público interesado las directrices generales sobre gobierno corporativo que se apliquen en la organización.

El Código de Ética establece el referente institucional de la conducta personal y profesional que todos los trabajadores de la empresa, independientemente del cargo o función que ocupen, deben tener como un patrón en el manejo de relaciones internas y con los grupos de interés.

Uno de los compromisos adquiridos por el equipo de dirección, es la implementación del sistema de gestión de seguridad e la información con el fin de obtener los siguientes beneficios.

- **Aspecto organizacional:** El registro de las actividades permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles y probar la diligencia razonable de sus administradores.
- **Aspecto legal:** El registro permite demostrar que la organización observa todas las leyes y normativas aplicables al alcance.
- **Aspecto funcional:** Obtención de un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección. Garantiza también una mejor disponibilidad de los materiales y datos.

- **Aspecto comercial:** Los socios, los accionistas y los clientes se tranquilizan al constatar la importancia que la organización concede a la protección de la información.
- **Aspecto financiero:** Reducción de los costos vinculados a los incidentes.
- **Aspecto humano:** Mejora la sensibilización del personal hacia la seguridad y a sus responsabilidades en la organización.

5.3 Responsabilidad y Autoridad.

A continuación se expone la siguiente ilustración la cual indica la estructura jerárquica organizacional, de tal manera que se pueda establecer las responsables para cada autoridad.

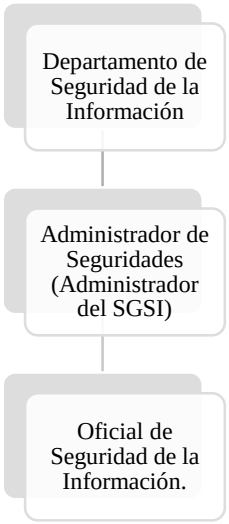


Figura 40: Diagrama jerárquico (ejemplo).

Fuente: Autor.

5.3.1 Responsabilidad del representante de la Dirección.

El rol de representante de la Dirección para el SGSI, es asumido por el Jefe de Unidad de Gestión de tecnología, quien además de sus responsabilidades por el cumplimiento de las estrategias, objetivos y resultados, es responsable de:

- Asegurar que los procesos establecidos para cumplir los requisitos de Seguridad de la Información, se establecen, implementan, mantienen y mejora.
- Asegurar que en el sistema de gestión de seguridad de la información, se definen e implementan acciones necesarias para su articulación con el sistema de calidad único de la empresa.
- Asegurar y evaluar la eficiencia del Sistema de Gestión de Seguridad de la Información y su mejora continua, así como reportar los resultados de las medidas de desempeño, relacionadas con los procesos, la conformidad de los controles, la retroalimentación de las partes interesadas y las auditorias.
- Asegurar que se promueva y se entienda, la importancia de la Seguridad de la Información a través del cumplimiento de los requisitos de la norma.
- Asignar los recursos requeridos para facilitar la implementación y sostenimiento del Sistema de Gestión de Seguridad de la Información.
- Informar a la alta dirección el desempeño del sistema de gestión y de cualquier necesidad de mejora.

5.3.2 Responsabilidad del Administrador del Sistema de Gestión.

- Asesorar y coordinar el establecimiento y desarrollo de las estrategias de aseguramiento y mejoramiento del sistema de Seguridad de la Información.
- Asesorar y coordinar la elaboración y ejecución del programa de auditorías internas.
- Diseñar y asesorar el cumplimiento del programa de formación para el personal como auditores internos.
- Promover la aplicación de mejores prácticas para la gestión documental de sistema de gestión de Seguridad de la Información.
- Asesorar en la gestión de Acciones Correctivas y Preventivas.
- Asesorar en las metodologías a aplicar para las revisiones gerenciales del sistema de gestión de Seguridad de la Información
- Coordinar los procesos de certificación del sistema de gestión de seguridad de la información.

5.3.3 Responsabilidad del personal de la organización.

- Asegurar el cumplimiento de los estándares y directrices del sistema de gestión de Seguridad de la Información, en ejecución de su trabajo diario.

- Evaluar permanentemente el desempeño individual frente a los aspectos de Seguridad de la Información y establecer acciones de mejora.
- Estar comprometidos con el SGSI haciendo vigías en seguridad de la información, reportando y gestionando permanentemente fallas o incidentes.
- Identificar oportunidades de mejoramiento del SGSI de la organización.
- Mantener una adecuada actitud de servicio al cliente, durante el desarrollo de los productos y servicios que estén a su cargo, de conformidad con las políticas establecidas por la organización.
- Actualizar los procedimientos internos para mejorar alineado con la política y objetivos del SGSI.

6. Gestión de Riesgos.

En cada proceso se identifica y se gestiona los riesgos de acuerdo con lo establecido por la organización a través de la Unidad de Gestión de Riesgos – UGR, de la misma manera, para asegurar la efectiva interacción de los procesos, el seguimiento de medición de los resultados, se trabaja con el enfoque de PHVA, que se evidencia en la estructura para el Control de la Gestión (ECG), en la que se

definen planes, programas, recursos, reportes y escenarios de seguimiento periódico (diario, semanal, mensual, trimestral, anual) de objetivos, metas e indicadores de la

gestión, permitiendo identificar de manera continua oportunidades de mejoramiento del sistema.

El marco normativo de gestión de riesgos, define los criterios para evaluar los riesgos, mediante la identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos de la información, para los cuales se realiza el análisis cualitativo de riesgos, utilizando la metodología MAGERIT para este fin, en la cual se valoran las probabilidades de ocurrencia y el impacto en la perspectiva de personas, económica, ambiente, imagen y cliente.

La política general de riesgos, define que los riesgos catalogados como altos (H), muy altos (VH) y medio (M), deben ser tratados y generar un plan de acción que permita que estos riesgos se encuentren en la categoría de Bajos (L), mediante la definición de una estrategia de mitigación: Aceptar o transferir para tratar amenazas y/o oportunidades, mitigar y eliminar para tratar las amenazas o explotar para tratar las oportunidades.

Debido a que el riesgo informático no puede llegar a ser mitigado en su totalidad se considera que a través de una adecuada gestión de riesgos, es posible llegar a obtener un porcentaje de exposición mínima ante incidentes de seguridad que puedan afectar la seguridad de la información.

Para que se pueda gestionar los riegos de manera eficiente y correcta se debe de considerar el desarrollo de los elementos descritos en la siguiente ecuación.

ECUACIÓN PARA LA GESTIÓN DE RIESGO.

$$Gestión\ de\ Riesgos = Análisis\ de\ riesgos + Tratamiento\ de\ riesgos$$

Figura 41: *Ecuación para la gestión de riesgos.*

Fuente: (Instituto Ecuatoriano de Normalización, 2010)

Elaborado por: Autor.

Para la revisión de la metodología de análisis y gestión de riesgos, revisar el anexo 9.

6.1 Declaración de aplicabilidad.

La declaración de aplicabilidad es la principal documentación requerida por la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011. La importancia de constituir este documento es porque dentro del mismo se expondrán todos los objetivos de control seleccionados del Anexo A, de la norma, así como sus respectivas exclusiones, los cuales van a ser utilizados para mitigar los riesgos existentes (Ver Anexo 3).

7. Revisión por la dirección.

La Revisión por la Dirección se realiza de acuerdo con lo establecido en el Procedimiento de Revisión por la Dirección, que se encuentra a su vez alineado con el Procedimiento de Revisión por la dirección de la organización.

El Sistema de Gestión de Seguridad de la Información debe ser evaluado una vez al año por el Jefe de unidad de Gestión de Tecnología a través de la Revisión por la Dirección realizada en una de las sesiones de comité de la unidad.

La Revisión por la Dirección incluye la toma de decisiones sobre acciones necesarias para el mejoramiento de los procesos y las capacidades para alcanzar resultados de eficiencia, eficacia y efectividad. Esto incluye el análisis de los resultados de la retroalimentación de las partes interesadas (Grupos de interés), el desempeño de los procesos, el cumplimiento de las especificaciones, los hallazgos de auditorías, las acciones correctivas y preventivas, y los cambios que se pueden afectar el Sistema de Gestión de Seguridad de la Información.

8. Mejora del SGSI.

8.1 Auditoría Interna.

Para determinar si los procesos del sistema de gestión de seguridad de la información son conformes con las disposiciones planificadas y con los requisitos de la norma técnica NTE INEN-ISO/IEC 27001:2011, se establece la realización de un ciclo de auditorías periódicas, de tal manera que se pueda verificar.

- El cumplimiento de los requisitos de la norma.
- El cumplimiento de los requisitos de seguridad.

- Que los requisitos se tengan implantados y se mantengan de manera efectiva.
- Que los requisitos implantados, den el resultado esperado.

Se debe planificar un programa de auditorías, teniendo en cuenta el estado e importancia de los procesos y áreas a auditar, asi como los resultados de las auditorias previas.

La selección del equipo de auditores y la dirección de las auditorias deben de garantizar la objetividad e imparcialidad del proceso de auditoría. *Los auditores no deben de auditar su propio trabajo.*

El responsable del área de auditoría debe velar por que se realicen acciones para eliminar, sin demoras indebidas, las desconformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones realizadas y los informes de los resultados de la verificación.

8.2 Seguimiento y medición.

Entre los mecanismos definidos está el seguimiento y la gestión a los incidentes de seguridad de la información, según el procedimiento Manejo

de Incidentes de Seguridad de la Información y el nivel de Aseguramiento de Seguridad de la Información.

Para medir la eficacia del SGSI, la efectividad de los controles y en general el desempeño del sistema, se implementan actividades de seguimiento y medición.

Para medir el nivel de eficacia de las acciones de mejora implementadas, es importante hacer una verificación del cumplimiento de las acciones de mejora establecidas, confirmando la eliminación de la causa raíz y en dado caso de evidenciar el incumplimiento, se debe justificar y examinar las causas del desempeño, el análisis del desempeño y las acciones de aseguramiento. Lo anterior, se puede confrontar en el listado maestro de acciones correctivas y preventivas del SGSI. Así mismo, el seguimiento a la ejecución de estas actividades se realiza a través de este listado, donde se puede hacer trazabilidad a las acciones que se encuentran cerradas a tiempo, cerradas con atraso, abiertas a tiempo o con atraso, en ejecución, o por iniciar.

Otra forma a través de la cual se podrá evidenciar la eficacia de las acciones, es a través de la repetición en cuanto a la ocurrencia de hallazgos independientemente de la fuente (Auditorias, revisiones por la dirección, entre otras)

Es fundamental, diferenciar bien las acciones correctivas de las preventivas. En este aspecto es importante revisar cuantas acciones

correctivas hay con respecto a las preventivas y determinar si hay inclinación positiva hacia la prevención más que a la corrección.

8.3 Acciones Correctivas

La industria química deberá identificar todas las no conformidades, ésto incluye determinar las causas de las no conformidades ya sean estas vulnerabilidades, riesgos o daños ocasionados.

De la misma manera es necesario evaluar la necesidad de acciones y que estas aseguren que las no conformidades vuelven a ocurrir, se debe determinar e implementar la acción correctiva necesaria y registrar los resultados de la acción tomada

Todas las acciones correctivas aplicadas deberán de ser debidamente registradas por la organización.

8.4 Acciones Preventivas.

La industria química deberá identificar las no conformidades potenciales y sus causas, ésto incluye evaluar la necesidad de acciones para impedir que las no conformidades ocurran y determinar e implementar las acciones preventivas necesarias.

Todas las acciones preventivas aplicadas deberán de ser debidamente registradas por la organización.

Manual de Gestión de Seguridad de la Información de una industria Química.		
Sistema de Gestión de Seguridad de la Información.		
CODIGO. **EC-155**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

9. Bibliografía.

Sistema de Gestión de Seguridad de la Información (SGSI). Requisitos. Guayaquil, Ecuador. 2015 (NTE INEN-ISO/IEC 27001:2011)

Revisó.	**Aprobó.**
Líder SGSI.	**Jefe de Seguridad de la Información.**

ANEXO 3: DECLARACIÓN DE APLICABILIDAD.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

DECLARACIÓN DE APLICABILIDAD.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Tabla de Contenido.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. EC-158	ELABORADO. 20/01/2015	Versión. 01

1. Objetivo.

A través de este documento se expresa formalmente las decisiones de la Gerencia del Proyecto SI, con relación al tratamiento de los riesgos que se realizará en respuesta al análisis de riesgos y diagnósticos de conformidad con la norma técnica NTE INEN-ISO/IEC 27001:2011, realizado en el marco del establecimiento del Sistema de Gestión de Seguridad de la Información.

2. Objetivos de Control y Controles seleccionados para el Tratamiento de Riesgos.

A continuación en la (Tabla #32), se presentan los objetivos de control y controles que han sido seleccionados para ser implementados en la entidad.

2.1 Selección de controles de la norma técnica NTE INEN-ISO/IEC 27001:2011

Tabla 30: Controles de seguridad aplicados en la organización.

A.5 POLITICA DE SEGURIDAD.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.5.1 Política de Seguridad de la Información. Objetivo: brindar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.	Cumplimiento de la Política.	Todos los usuarios deben conocer la Política y las implicaciones del no cumplimiento.
	Responsables de Actualizarla y divulgarla.	Las responsabilidades y funciones para mantener actualizada y divulgada la Política se deben incluir dentro del manual de responsabilidades de las áreas asignadas.
	Aprobación.	Las actualizaciones deben ser aprobadas por el comité Gerencial.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.6 Organización interna. Objetivo: Gestionar la seguridad de la información dentro de la organización.	Compromiso de la Dirección.	La Alta Dirección o a quien delegue deberá asegurar los recursos financieros, humanos y logísticos para el logro de los objetivos del SGSI. El Comité Gerencial realizará seguimiento trimestral sobre el logro de los objetivos del SGSI.
	Coordinación.	Asignar un responsable de coordinar las actividades a nivel de la entidad relacionadas con la Seguridad de la Información y sus actores (dueños, responsables de activos, usuarios, custodios, entre otros)
	Asignación de responsabilidades en todos los niveles de la entidad.	La responsabilidad deben estar claramente definidas y documentadas en el manual de funciones de cada cargo.
	Autorización de uso de recursos.	Procedimiento que establezca los pasos que se deben cumplir antes de poner en producción un nuevo servicio o infraestructura tecnológica.
	Acuerdos de confidencialidad.	Todo acuerdo de confidencialidad deberá incluir la información que no puede ser divulgada, la vigencia del acuerdo, los derechos de propiedad de la misma y cuando aplique, el derecho de auditar las acciones que se hagan sobre la misma, así como las implicaciones por el no cumplimiento del acuerdo.
	Contactos con autoridades y/o entidades.	Establecer acuerdo de mutuo apoyo, documentar las personas de contacto y el protocolo a seguir en caso de necesitar su intervención.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Grupos de Interés.	El especialista o ingeniero de seguridad de la información deberá estar registrado como punto de contacto entre la entidad y las organizaciones especializadas de seguridad de la información y proveedores o fabricantes de la tecnología implementada por la industria química para mantenerse actualizado de las posibles vulnerabilidades y riesgos, deberá definir y poner en ejecución el plan preventivo o correctivo para reducir la probabilidad de materialización de un evento no deseado por su impacto negativo (incidente).
	Revisiones Independientes.	Control interno realizará anualmente una auditoría sobre la efectividad del sistema y reportará al Comité Gerencial los hallazgos y recomendaciones para establecer los planes de mejora del SGSI.
	Identificación de riesgos por conexiones a terceros.	La autorización de compartir información con terceros o permitir la conexión en la red interna de la Entidad debe tener como soporte el análisis de riesgos realizados.
	Manejo de información de clientes.	La entidad por ser fuente y operador de la información de sus clientes debe garantizar la confidencialidad e integridad de la misma por lo tanto deberá implementar acuerdos de confidencialidad y aplicar los controles de acceso establecidos en los ítems de Dominios: Gestión de Comunicación y Operaciones (Gestión de Seguridad de Red) y Control de Acceso.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.7 GESTIÓN DE ACTIVOS		
Objetivo de Control.	**Control.**	**Aplicación.**
A.7.1 Responsabilidad por los activos. **Objetivo:** Lograr y mantener la protección apropiada de los activos organizacionales.	Inventario de activos.	El responsable o dueño del proceso verificará, mínimo cada semestre o cuando haya algún cambio, que el inventario esté actualizado en la herramienta de Gestión de Riesgos (ERA) y dejará evidencia de su gestión, mediante acta.
	Propiedad de los activos.	Todo activo tiene asignado un dueño o responsable quien garantizará que este apropiadamente clasificado, y verificará si las restricciones de acceso son las adecuadas.
	Uso aceptable.	Cada tecnología, servicio o recurso tendrá documentado las reglas de uso adecuado.
A.7.2 Clasificación de la información. Objetivo: Asegurar que la información reciba un nivel apropiado de protección.	Directrices de Clasificación.	Los activos serán identificados de acuerdo con la guía establecida en el sistema ERA, bajo los tres atributos de seguridad: Confidencialidad, disponibilidad e integridad, así como la criticidad que tiene para el proceso o sistema.
	Etiquetado y Manipulación de Información.	Información en papel debe de estar marcada con una etiqueta adhesiva o sello que identifique su clasificación. Información almacenada en medios electrónicos debe tener una marca de agua o incluir en el pie de página su clasificación. Información de salida clasificada como reservada o altamente confidencial debe estar protegida por sobre sellado y marcado como confidencial y este a su vez debe ser guardado en otro sobre sin etiquetar.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.8.1 Antes de la relación laboral. Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entiendan sus responsabilidades y sean adecuados para los roles que se los considera, y reducir el riesgo de hurto, fraude o uso inadecuado de las instalaciones.	Concurso ocupar vacante.	Todo proceso de selección de personal, desde su inicio, debe hacer explícito las responsabilidades propias del cargo como las relaciones con la seguridad de la información, así como las posibles sanciones por el no cumplimiento.
	Responsabilidades.	Las funciones y responsabilidades, como el perfil requerido para desempeñar el cargo o prestar sanciones, deben estar definidas y documentadas de acuerdo con el marco normativo de seguridad de la información.
	Proceso de selección.	Se debe tener una lista o base de datos de todos los candidatos que van a ocupar vacante que registre la información de datos personales, educación, experiencia, certificaciones, referencias personales, laborables, entre otros. El acceso y manejo de dicha información debe cumplir con la Ley Ecuatoriana de Habeas Data.
	Requisitos mínimos de los candidatos.	Debe existir una lista de verificaciones de los requisitos que debe cumplir los aspirantes a un cargo, contrato o acuerdo. Dentro de los requisitos se debe incluir la comprobación de la hoja de vida, las certificaciones académicas, etc.
	Acuerdos de Confidencialidad-	Como parte de su obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo el cual establecerá sus obligaciones.

Objetivo de Control.	Control.	Aplicación.
A.8.2 Durante la relación laboral. Objetivo: Asegurar que todos los empleados, contratistas y usuarios por tercera parte tengan conciencia sobre las amenazas y problemas relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y que estén preparados para brindar apoyo a la política de seguridad de la información organizacional en el curso de su trabajo normal, y para reducir el riesgo de error humano.	Responsabilidades de la Dirección.	Dentro de las funciones. (Superintendentes, Delegados, Directores, Coordinadores y Jefes de Oficinas) deben estar incluidas las funciones que permitan garantizar que los funcionarios, contratistas y demás usuarios cuenten con una guía de buen uso de los recursos informáticos, conocen y están incluidas dentro de sus funciones la seguridad de la información, están capacitados y entrenados para asumir la responsabilidades asignadas y son actualizados en el modelo normativo (política, directrices, normas, procedimientos)
	Capacitación y entrenamiento.	Todos los empleados de la entidad, contratista y usuarios deben percibir, además de los requeridos para desempeñar el cargo, capacitación y entrenamiento sobre seguridad de la información y ser actualizados sobre el modelo normativo que sean relevantes para la función de su trabajo.
	Proceso Disciplinario.	Debe existir un proceso formal disciplinario para empleados que han cometido una acción en contra de la seguridad de la información.
A.8.3 Terminación o cambio de la relación laboral. Objetivo: Asegurar que los empleados, contratistas y usuarios por tercera parte abandonen una organización o cambian de empleo de una manera ordenada.	Responsabilidades.	La responsabilidad que siguen vigentes después de terminar la relación contractual y su vigencia deben estar explícitamente definidas y haber sido excluidas desde un inicio en el contrato o acuerdo aceptado y firmado por el funcionario, contratista o tercera parte.

Objetivo de Control.	Control.	Aplicación.
	Entrega del Cargo	Debe existir un procedimiento para entregar el cargo ya sea por terminación del contrato o por cambio de cargo
	Entrega de Activos.	Mediante acta de entrega el responsable de recibir debe registrar todos los activos a cargo de quien entrega, cuales fueron efectivamente definidos, y cualquier observación. Dentro de la entrega deben incluir los documentos de identificación de la entidad, las tarjetas o llaves de acceso a los activos de información o al centro de cómputo.
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO.		
A.9.1 Áreas seguras. Objetivo: Evitar el acceso físico no autorizado, el daño e interferencias a las instalaciones e información de la empresa.	**Centro de Computo**	
	Control de Acceso.	Procedimientos de autorización y control de ingreso al Centro de Cómputo.
	Seguridad Perimetral.	Mantener activos permanentemente los controles de ingreso a áreas seguras. Su desactivación deberá generar algún registro del hecho.
	Sistema contra incendios.	Verificar periódicamente que el sistema es efectivo.
	Sistema de Control de Factores Ambientales.	Sistema de protección contra humedad, inundación o cargas electromagnéticas implementados y monitoreados

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Instalaciones.	
	Ingreso.	Autorización del ingreso a personal ajeno en el sistema de control de ingreso de visitantes, incluyendo datos como el motivo de la visita. Acompañamiento del personal ajeno por parte de quien lo autoriza, si se dirige a un área de acceso restringido.
	Identificación.	Identificación visible de toda persona dentro de la entidad (carnet o escarapela de identificación). Cualquier otro funcionario es responsable de solicitar a un extraño que se identifique.
	Guía de comportamiento.	Guía de comportamiento dentro de las instalaciones la cual debe ser conocida por los visitantes.
	Amenazas Externas.	Evaluación de riesgos por condiciones externas, como atentados, incendios, inundaciones, etc. Y establecimiento de un plan preventivo y/o correctivo. Los materiales peligrosos y combustibles (cajas, papelería, etc.) almacenados en lugares distantes de las áreas seguras. Los suministros solo deben permanecer mientras se necesiten.
	Trabajo en áreas Seguras.	Procedimiento para la autorización y ejecución de trabajos en áreas seguras como en el centro de cómputo.
	Áreas de carga y descarga de insumos.	Recepción y almacenamiento de materiales peligrosos y combustibles (cajas, papelería, etc.) en lugares distantes a las áreas seguras.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.9.2 Seguridad de los equipos. Objetivo: Evitar perdida, daño, robo o puesta en peligro de los activos e interrupciones de las actividades de la organización.	Protección de equipos.	Requerimiento obligatorio de contraseña para la inicialización del sistema (en el proceso de preboot). Conexión de los equipos a tomas de corriente regulada. Prohibición de comer y fumar en áreas donde se encuentre equipos de cómputo.
	Instalación de suministros	Plan de ejecución de mantenimientos preventivos a la infraestructura de suministro de energía eléctrica, aire acondicionado, contra incendio, etc.
	Seguridad del cableado.	Las acometidas eléctricas separadas del cableado de comunicación (voz, datos), protegidas e identificadas.
	Mantenimiento de equipos.	Ejecución del plan de mantenimiento preventivo y correctivo de PCs, servidores y equipos de comunicación.
	Seguridad de los equipos fuera de las instalaciones.	Cifrado de los discos de los equipos portátiles.
	Reutilización o retiro de equipos.	Borrado efectivo de la información contenida en los equipos declarados como obsoletos o que van a ser reutilizados mediante métodos seguros como reescritura de información con basura o blancos, formateo seguro, o utilización de imanes.
	Salida de material de propiedad de la entidad.	Procedimiento formal para controlar la salida de equipos.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.10.1 Procedimientos operacionales y responsabilidades. Objetivo: Asegura la operación correcta y segura de las instalaciones de procesamiento de información.	Documentación de los procedimientos de operación.	Procedimientos documentados de operación, administración y configuración de Firewasll, Switches, Servidores, Herramientas de Backup, equipos de comunicación y tecnología de seguridad.
	Gestión de cambios.	Procedimiento de control de cambios para el ingreso de nuevos sistemas al ambiente productivo o cambios mayores.
	Segregación de funciones.	Actividad de administración y de auditoría de los sistemas deben ser asignadas a personal diferente de operación.
	Separación de ambientes.	Ambientes diferentes al de producción para las actividades de desarrollo y pruebas de los sistemas de información.
A.10.2 Gestión de la prestación del servicio por tercera parte. Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y prestación del servicio en línea con los acuerdos de prestación de servicios por una tercera parte.	Provisión.	Verificación del cumplimiento de los niveles de servicios y los requerimientos de seguridad establecidos en los contratos de prestación de servicios por terceros.
	Supervisión y revisión.	Revisión mensual de los reportes sobre la prestación de los servicios. El contenido del reporte acordado entre las partes, incluyendo como mínimo los indicadores de cumplimiento de los niveles de servicio, los problemas o incidentes presentados y las acciones correctivas implementadas.
	Gestión de cambios.	Procedimiento de Gestión de Cambios aplicado para cualquier cambio al ambiente productivo (adopción de nuevas tecnologías, nuevos productos, cambio de controles, sistemas, etc.)

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.10.4 Protección contra códigos maliciosos y móviles. Objetivo: Proteger la integridad del software y la información.	**Controles contra código malicioso.**	
	Norma de uso legal de software.	Prohibición de uso de software no autorizado y/o licenciado.
	Generación de cultura.	Inclusión en el plan de cultura de sensibilizar sobre los efectos de bajar archivos o software de internet o medios removibles no autorizados y las medidas de protección.
	Control de utilización de software.	Bloqueo de ejecución de software no autorizado mediante la definición de perfiles de aplicación de la herramienta Secuware.
A.10.5 Copias de Seguridad. Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.	Copias de seguridad.	Ejecución de copias de seguridad tanto de datos, programas y configuraciones de los sistemas de información de servidores y PCs de usuarios, dispositivos de tecnología de información clasificados como críticos de acuerdo con la valoración de activos de información y siguiendo el procedimiento: “Respaldo de datos de la infraestructura tecnológica”
A.10.6 Gestión de la seguridad de redes. Objetivo: Asegurar la protección de la información de las redes y la protección de la infraestructura de soporte.	Controles de red.	Definición de responsabilidades y segregación de actividades de administración y operación. Verificación de cumplimiento de nivel de servicios.
	Seguridad de los servicios.	Identificación e inclusión de las características de seguridad (autenticación, cifrado y control de acceso), los niveles de servicios y los requisitos de gestión de todos los servicios de red en los acuerdos de servicios establecidos con los proveedores.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.10.7 Manejo de medios. Objetivo: Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.	Gestión de medios extraíbles.	Definición de criterios de autorización de uso de medios removibles (Cintas, CDs, DVD, USB) y medidas de protección física, control de uso de los medios, verificación de la confiabilidad del medio y copias de respaldo.
	Eliminación de medios.	Eliminación segura de información cuando se den de baja o van a ser reutilizados con otro fin (aplica también para impresoras).
	Procedimientos de manipulación de la información.	Procedimiento para la manipulación y almacenamiento de la información.
	Seguridad de la documentación del sistema.	Nombramiento de un responsable de la administración de la documentación de los sistemas. Salvaguarda de estos documentos bajo llave y procedimientos de control y autorización de uso.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y el software que se intercambia dentro de la organización y con cualquier entidad externa.	Políticas y procedimientos de intercambio de información.	Política que establezca responsabilidades, medios de protección para el intercambio de información (hablada, escrita o electrónica), tanto al interior de la entidad como con otras entidades.
	Acuerdo de intercambio.	Acuerdos formales para el intercambio de información y software entre la Organización y terceros que contemple responsabilidades, uso aceptable de la información, seguridad de empaque y envío, derechos de uso y propiedad.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Soportes físicos en tránsito.	Envío de medios o información mediante mensajería certificada, entrega en mano por mensajeros confiables o transporte seguro. Todos los medios que contengan información clasificada como crítica debe ser empacada en forma segura (contenedores cerrados, sobres de seguridad.)
	Mensajería electrónica.	Guía de uso adecuado del correo. Implementación de mecanismos que garanticen la no repudiación, confidencialidad e integridad del contenido. Control del tamaño y tipo de archivos adjuntos. Control anti-spam.
	Sistemas de Información	Autorización de acceso por el propietario o responsable del sistema previa evaluación de riesgos. Sistema de autenticación fuerte. Activación de logs.
A.10.9 Servicios de comercio electrónico. Objetivo: Garantizar la seguridad de los servicios de comercio electrónico su utilización segura.	Información puesta a disposición pública.	Protección contra escritura o eliminación no autorizada de información publicada en internet o de los sistemas de información. Evaluación de la información a publicar de acuerdo con las leyes Ecuatorianas.
A.10.10 Monitoreo. **Objetivo:** Detectar actividades de procesamiento de la información no autorizada.	Registro de auditorías.	Grabación de las actividades de los usuarios, excepciones y eventos de la seguridad (intentos de ingreso fallidos, ingresos exitosos, modificación o eliminación de información, etc) Monitoreo del uso de los sistemas de información que permita detectar intentos de acceso indebidos.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Protección de la información de los registros.	Acceso restringido al log de auditoria. Toma de copias de respaldo.
	Registros de administración y operación.	Registro de los cambios a la infraestructura o configuración del sistema o excepciones de operación
	Registros de fallos.	Bitácora de fallas presentadas y acciones correctivas realizadas.
	Sincronización del reloj.	Sincronización del reloj de todos los equipos (PCs, servidores, dispositivo de tecnología de información) con el servidor oficial de tiempo. No se debe permitir el cambio por usuarios finales, para sistemas que proporcionen esta restricción se debe de garantizar la actualización automática mediante el proceso de ejecución de sincronización. Registro en el log de los cambios realizados, sin importar el tipo de usuario.
A.11 CONTROL DE ACCESO.		
A.11.1 Requisitos del negocio para el control de acceso. Objetivo: Controlar el acceso a la información.	Política de control de acceso.	Autorización del acceso a la información y/o sistemas de acuerdo a las necesidades para desempeñar sus funciones. Aplicación del principio de: “Todo lo que no está permitido explícitamente, está prohibido”
A.11.2 Gestión de acceso de usuarios. Objetivo: Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado de información.	**Registro de usuario**	
	Procedimiento de Administración.	Procedimiento de administración de usuarios definido e implementado que contemple tanto la creación como eliminación de los usuarios y la asignación de permisos.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Identificadores de usuarios.	Identificación de usuario único. Cuando se requiera un identificador de usuario grupal éste debe ser justificado, autorizado y ser documentado.
	Gestión de privilegios.	Asignación de privilegios a los individuos según los principios de "necesidad de su uso" y por "caso por caso" y consistente con la política de control de acceso. Asignación de privilegios por el propietario de sistema o líder funcional
	Gestión de contraseña de usuario.	
	Identidad del usuario.	Procedimiento para la asignación y modificación de contraseñas que garantice la autenticidad del usuario.
	Confidencialidad de las contraseñas	Las contraseñas almacenadas en forma cifrada y entrega en forma segura al usuario (propietario).
	Cambio obligatorio de contraseñas.	Manejo de vigencia de la contraseña en los sistemas y solicitud de cambio de la misma cuando éste vence, o cuando se le asigna por primera vez o por reasignación.
	Contraseñas predefinidas.	Cambio de las contraseñas que vienen definidas por el fabricante antes de que el sistema inicie su vida productiva.
	Revisión de los derechos de acceso.	Revisión semestral de los derechos asignados a los usuarios o cada vez que haya un cambio de rol usuario. Revisión trimestral de los usuarios con derechos especiales. Notificación y registros de cualquier inconsistencia al responsable del área de seguridad.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.11.3 Responsabilidad de los usuarios. **Objetivo:** Evitar el acceso a usuarios no autorizados, y el hurto o la puesta en peligro de información y de instalación de procesamiento de información.	**Uso de contraseñas.**	
	Norma restricción de compartir contraseñas.	Regla que establece que la contraseña es personal e intransferible.
	Cambio de contraseñas por el usuario.	Definición de la responsabilidad de cambiar la contraseña cada vez que exista un indicio de que ha sido comprometida o cuando se le ha asignado por primera vez o ha sido reasignada.
	Guía de asignación de contraseñas no obvias.	Pautas para asignar una contraseña no obvia y fácil de recordar.
	Contraseñas seguras.	Activación en los controladores de dominio de la factibilidad de validación de contraseñas (longitud mínima, combinación de tipo de caracteres, claves diferentes al ID del usuario, etc.) e implementación para los demás sistemas de algoritmos de validación de contraseñas seguras (no obvias, historial de contraseñas, etc.)
	Equipo de usuario desatendido.	
	Bloquear sesión de trabajo.	Bloqueo de los equipos cada vez que el usuario no se encuentre en su puesto de trabajo.
	Manejo de tiempos	Activación en los controles de dominio de las políticas de control de sesiones (time out de sesión).
	Política de puesto de trabajo.	Escritorios libres de documentación, dispositivos o cualquier otro medio que contenga información que pueda poner en peligro el activo mientras no se requiera para el desarrollo de sus actividades.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.11.4 Control de acceso a redes. **Objetivo:** Impedir el acceso no autorizado a servicios en red.	Política de uso de los servicios de red.	Establecimiento del responsable de autorizar el uso de los servicios ofrecidos y la conexión a redes tanto internas como externas.
	Autenticación de usuario para conexiones externas.	Mecanismos de autenticación (al menos mediante contraseña) para conectarse remotamente a la red de la entidad para usar servicios no públicos.
	Identificación de equipos en la red.	Autenticación de equipos que se conecten a la red interna de la entidad mediante certificados digitales del equipo.
	Diagnostico remoto y protección de puertos.	
	Diagnóstico.	Utilización de productos seguros para la conexión a dispositivos para diagnosticar configuraciones como ssh, https. Aprobación oficial de las herramientas de acceso remoto.
	Protección física de puertos.	Gabinetes cerrados con llave, done están los equipos de red.
	Registro de eventos.	Autenticación ante el sistema para los usuarios y registros en el log de ingresos de esta actividad, así como de cambios físicos a la configuración de lo equipos de red.
	Segregación de las redes.	Segregación de las redes con base en el diseño de red segura aprobada por la entidad.
	Control de la conexión a la red.	Los responsables de los servicios informáticos deben autorizar las solicitudes de conexiones a sistemas, redes o servicios.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.11.5 Control de acceso al sistema operativo. **Objetivo:** Evitar el acceso no autorizado a los sistemas operativos.	Procedimientos seguros de inicio de sesión.	Despliegue de un mensaje en los sistemas, que advierta que solo está disponible para usuario autorizaos y las implicaciones de uso no autorizado. Restricción de presentación de información en los sistemas que sirva de base para identificar datos del posible usuario, sistema operativo, etc.
	Identificación y autenticación de usuario.	Asignación de un identificador único para todo usuario que se desconecte al sistema operativo. Norma que prohíba el uso de identificador de usuario compartido.
	Sistema de gestión de contraseña.	Aplicación de los mismos controles de gestión de contraseñas de usuarios y uso de contraseñas (ítem 11.2). Establecimiento de un tiempo máximo para ingresar los datos de identificación y autenticación.
	Uso de los recursos del sistema.	Restricción del uso de utilitarios del sistema a personal autorizado y para las actividades específicas justificadas. Registro en el log de la utilización del sistema y monitoreo del mismo.
	Desconexión automática de sesión.	Desactivación automática de sesiones inactivas durante un tiempo determinado.
	Limitación del tiempo de conexión.	Establecimiento de tiempo máximo de conexión y desactivación de la sesión una vez que se cumpla.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
A.11.6 Control de acceso a las aplicaciones y a la información. **Objetivo:** Evitar el acceso no autorizado a la información contenida en los sistemas de información.	Restricción del acceso a la información.	Menús de opciones en los sistemas de información que permiten implementar control de acceso a su funcionalidad e información.
	Aislamientos de sistemas sensibles.	Asignación de recursos exclusivos para sistemas de información sensible. Cualquier excepción debe ser documentada. Protección de los equipos de cómputo que los soportan mediante un firewall (ubicados en una DMZ)
A.11.7 Computación móvil y trabajo remoto. **Objetivo:** Garantizar la seguridad de la información cuando se usan instalaciones de computación móvil y trabajo remoto.	Ordenadores portátiles y comunicaciones móviles.	Guía de protección física de los equipos. Cifrado de información. Autorización de conexión a la red solo si no está contaminada (control de código malicioso)
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.		
A.12.1 Requisitos de Seguridad de los Sistemas de Información. **Objetivo:** Garantizar que la seguridad es parte integral de los sistemas de información.	Análisis y especificación de los requisitos de seguridad.	Desde las especificaciones funcionales del sistema se deben identificar los requisitos de seguridad con el fin que sean considerados dentro de los criterios de adquisición, desarrollo o mantenimiento de software.
A.12.2 Procesamiento correcta en las aplicaciones. **Objetivo:** Evitar errores, perdidas, modificación no autorizada o mala utilización de la información en aplicaciones.	Validación de los datos de entrada.	Implementación de rutinas de validación datos (rango de valores tipo de campo, campos obligatorios, caracteres permitidos, etc.)
	Control de procesamiento interno	Implementación de rutinas de control de flujo de procesamiento, manejo de errores, integridad de información, puntos de recuperación de archivos.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Integridad de los mensajes.	Sistemas que generen correos deben garantizar la integridad del mismo.
	Validación de los datos de salida.	La información de salida debe ser suficiente para que el usuario pueda determinar su consistencia.
A.12.3 Controles criptográficos. **Objetivo:** Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.	Política de uso de los controles criptográficos	Establecer los criterios para la implementación de cifrado de la información
	Gestión de claves.	Procedimiento de generación, manejo y custodia de claves de cifrado.
A.12.4 Seguridad de los Archivos del Sistema. **Objetivo:** Garantizar la seguridad de los archivos del sistema.	Control de software en producción.	Aplicar procedimientos de control de cambios. Bitácoras de registro de actualizaciones e instalación de software. Copias de respaldo de sistema y del software (manejo de versiones).
	Protección de los datos de prueba del sistema.	Selección de datos de pruebas que reflejen la realidad sin que se utilicen datos de producción. Si por alguna razón los datos son tomados del ambiente de producción se debe preservar sus atributos de seguridad.
	Control de acceso al código de fuente de los programas.	Debe haber un responsable de administrar los programas fuentes. Los programas no deben residir en los ambientes de producción. El acceso a los programas fuentes deben de ser autorizados.
A.12.5 Seguridad en los procesos de desarrollo y soporte. **Objetivo:** Mantener la seguridad del software y de la información del sistema de aplicaciones.	Procedimientos de control de cambios.	Todo mantenimiento de sistemas o cambios de operación debe cumplir con el procedimiento de control de cambios.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	Control.	Aplicación.
	Revisión de técnicas de aplicaciones tras efectuar cambios en el sistema operativo.	Cuando se realicen cambios en el ambiente operativo (infraestructura, actualizaciones de sistema operación, etc.) se debe verificar que los sistemas de información o servicios no fueron afectados.
	Restricciones a los cambios en los paquetes de software.	Los cambios al software adquirido deben responder a una necesidad real. Se deben establecer acuerdos con el proveedor para que las nuevas versiones de software contengan los cambios realizados, verificar que efectivamente la nueva versión no está afectando la funcionalidad propia del cambio.
	Fugas de Información.	Revisión de código fuente para identificar instrucciones maliciosas (troyanos) que permitan posibles fugas de información.
	Externalización del desarrollo de software.	El contrato de desarrollo debe tener definido explícitamente la propiedad del software, los derechos de autor y el establecimiento de garantía de calidad. Se deben hacer revisiones exhaustivas del código para garantizar que cumple solo con la funcionalidad definidas y no contienen código malicioso.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información. **Objetivo:** Asegurar que los eventos de seguridad y las debilidades de seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	Notificación de eventos de seguridad de la información.	Reporte de incidentes de seguridad inmediatamente sean identificados de acuerdo con el procedimiento de Administración de Incidentes.
	Notificación de puntos débiles de la seguridad.	Reporte a la mesa de ayuda por todos los usuarios (funcionarios, contratistas y terceros) de cualquier debilidad observada y direccionada del requerimiento por parte de la mesa de ayuda a TI.
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información. **Objetivo:** Asegurar que se aplique el enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información	Responsabilidades y procedimientos.	El equipo de atención de incidentes debe tener claramente definida sus responsabilidades y el procedimiento a seguir en caso que se presenta algún incidente (denegación de servicio, contaminación de red por virus, pérdida de integridad o fuga de la información, etc.)
	Aprendizaje de los incidentes de seguridad de la información.	Se debe dejar registro de los incidentes presentados y documentar las causas, las acciones tomadas y los costos en que se incurrieron para que sea la base de análisis para establecer planes de acción para la prevención de nuevos incidentes.
	Recopilación de evidencias.	El equipo de respuesta a incidencias debe estar capacitado para recolectar las evidencias de forma que no se comprometa su admisibilidad legal. Las evidencias deben ser protegidas de moda que no se ponga en duda la integridad.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
Objetivo de Control.	**Control.**	**Aplicación.**
A.14.1 Aspectos de Seguridad de la Información, de la gestión de la continuidad del negocio. **Objetivo:** Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.	Inclusión de las seguridades de la información en el proceso de recuperación ante desastres.	Plan actualizado y probado. El plan debe tener en cuenta los requerimientos mínimos de seguridad.
	Continuidad del negocio y evaluación de riesgos.	El DRP debe responder a un análisis de riesgos que permita priorizar las actividades de recuperación.
	Pruebas, mantenimiento y reevaluación de planes de continuidad.	El plan de pruebas del DRP y su actualización debe ser el establecido en el DRP.
A.15 CUMPLIMIENTO.		
A.15.1 Cumplimiento de los requisitos legales. Objetivo: Evitar el incumplimiento de cualquier ley, obligación estatutaria, reglamentaria o contractual, y de cualquier requisito de seguridad.	Identificación de la legislación aplicable.	Con el apoyo de la oficina jurídica se debe definir, documentar y mantener actualizado todos los requerimientos legales, regulatorios, contractuales que sean importantes para cada sistema de información.
	Derechos de propiedad intelectual.	Política de conformidad de los derechos de autor de software. Guía de protección de derechos de autor.
	Protección de los documentos de la organización.	Clasificar los registros y documentos de la entidad (registros contables, logs, documentación técnica, etc.), establecer tiempos de retención y definir medios seguros de almacenamiento según su clasificación.

Objetivo de Control.	Control.	Aplicación.
	Protección de datos y privacidad de la información personal.	Cumplir con los requerimientos de la ley ecuatoriana de protección de datos. El acceso a información personal debe estar restringido a personal autorizado. Los datos deben ser almacenados en forma cifrada o controlar el acceso directo a la Base de Datos.
	Prevención del uso indebido de los recursos de tratamiento de la información.	Mensajes de advertencia de disuasión de no utilizar los recursos de tratamiento de la información para propósitos no autorizados.
A.15.2 Cumplimiento de políticas y normas de seguridad y cumplimiento técnico. **Objetivo:** Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.	Cumplimento de las políticas y normas de seguridad.	Auditorías internas anuales. Auditorías externas cada 3 años.
	Comprobación del cumplimiento técnico.	Revisión de las características de los sistemas de información y tecnología de comunicaciones. Pruebas anuales de vulnerabilidades.
A.15.3 Consideraciones de la auditoría de sistemas de información. **Objetivo:** Maximizar la eficacia del proceso de auditoría de sistemas de información y minimizar la interferencia desde y hacia éste.	Controles de auditoría de los sistemas de información.	Planeación y ejecución de auditoría técnica a los sistemas de información.
	Protección de las herramientas de auditoría de los sistemas de información.	Control de acceso a las herramientas y archivos de trabajo de auditoría.

Fuente: (Instituto Ecuatoriano de Normalización, 2010)**.**

Elaborado por: Autor.

3. Controles implementados actualmente.

Tabla 31: Controles implantados en la organización.

Objetivo de Control.	Control.	Aplicación.
Código disciplinario único. **Objetivo:** Establece los deberes, prohibiciones y sanciones que se aplican a los empleados de la organización. A continuación se presentan los ítems relacionados con la seguridad de la información del código.	Proporcionar datos inexactos o presentar documentos ideológicamente falsos u omitir información que tenga incidencia en su vinculación o permanencia en el cargo o en la carrera, o en las promociones de ascensos o para justificar una situación administrativa. Ocasionar un daño o dar lugar a perdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder. Nombrar o elegir, para el desempeño de cargos públicos, personas que no reúnan los requisitos constitucionales, legales. Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas.	Por ser tan extenso, los funcionarios no tienen presente los elementos claves del código. Se recomienda realizar campañas de concientización sobre los elementos más relevantes tomando como base los valores institucionales.
Código del Buen Gobierno.	**Anticorrupción.** **Artículo 14.** La organización se compromete a luchar contra la corrupción. **Artículo 15.** La organización está en contra de toda práctica corrupta. **Compromiso en la lucha antipiratería.** **Artículo 17.** La organización velará porque se respeten las normas de protección a la propiedad intelectual y los derechos de autor.	No ha divulgado.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	**Control.**	**Aplicación.**
Permisos de cambio.	La configuración de los equipos solo puede ser realizado en forma local por el usuario administrador o remotamente o local con usuario de red con permisos administración.	Usuarios esporádicos.
Inducción sobre funcionalidad de los sistemas.	Los usuarios reciben una semana de inducción sobre la funcionalidad del sistema.	No todos los sistemas de información tienen completa o actualizada la documentación lo que dificulta el proceso de inducción.
Cámaras de video.	Ubicada en diferentes sitios, en el día existe una persona que monitorea el circuito de cámaras, en la noche se graba y se revisa al día siguiente.	No existe un procedimiento o guía que permita saber qué hacer en caso de que se presente una situación anormal.
Comité de seguridad institucional.	Mensualmente se hace reuniones del comité donde participan representantes de las diferentes entidades y se genera recomendaciones las cuales son aplicadas en la entidad.	

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Declaración de Aplicabilidad.		
CODIGO. **EC-158**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

Objetivo de Control.	**Control.**	**Aplicación.**
Sistema contra incendios.	Se cuenta con dos sistemas: **Manual:** 22 gabinetes con mangueras hidrantes y extintores tipo BC ubicados en cada piso y en diferentes sitios, y 40 extintores más (16 tipo ABC, 3 BC, 16 Solkaflam, 1 CO2, 4 de Agua). **Automático:** Ubicado en el centro de cómputo, con sensores de humo y señales audiovisuales en caso de emergencia.	
Firewall Externo.	Check Point 4500, en alta disponibilidad, activo – activo. Funcionalidad implementada: Firewall, VPN, Antivirus, Antibot, Antispam, Control de Contenido.	
SSF (Secureware Security Framework)	Seguridad para el usuario final (PCs, portátiles, medios removibles.) Funcionalidades. Control de ejecución de aplicaciones. Cifrado de discos. Control de conexiones a USB.	

Objetivo de Control.	Control.	Aplicación.
Correlación de eventos.	RSA: Correlación de eventos (logs) de dispositivos de seguridad, de red, servidores, etc. y alerta de posibles amenazas.	En implementación.
Límite de tamaño buzón Outlook.	Tamaño máximo del buzón para funcionarios normales 57 MB, para los directivos 200 MB, si el buzón llega a su límite no permite el envío.	
Control de archivos adjuntos en correos.	El tamaño de archivos adjuntos (10 Mb), no se permiten enviar videos.	
Cláusula de confiabilidad de contratos con terceros.	Dependiendo del contrato la cláusula tiene diferente rotulo aunque el texto es similar.	
Identificación de expedientes.	Expedientes con información confidencialidad están identificados con color rojo.	
Numero de radicación.	Todo documento de entrada o salida se le asigna una etiqueta el cual incluye el número de radicación que lo identifica como único.	

Fuente: (Instituto Ecuatoriano de Normalización, 2010)**.**

Elaborado por: Autor.

4. Exclusiones sobre la norma técnica NTE INEN-ISO/IEC 27001:2011.

Tabla 32: Exclusiones de controles.

Objetivo de Control.	Control.	Aplicación.
A.10.9 Servicios de comercio electrónico. **Objetivo:** Garantizar la seguridad de los servicio de comercio electrónico, y su uso seguro.	Comercio Electrónico: (ISO/IEC 27001:2011) – clausula A.10.9.1).	No se realizan transacciones de comercio electrónico.
A.15.1 Cumplimiento de los requisitos legales.	**Reglamentación de los controles criptográficos:** (ISO/IEC 27001:2001 – Clausula 15.1.6)	Ecuador no tiene ninguna prohibición para el uso de software de cifrado.

Fuente: (Instituto Ecuatoriano de Normalización, 2010)**.**

Elaborado por: Autor.

ANEXO 4: CONTROL DE DOCUMENTOS Y REGISTROS.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento de control de documentos y registros.		
CODIGO. **EC-159**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

PROCEDIMIENTOS DE CONTROL DE DOCUMENTOS Y REGISTROS.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento de control de documentos y registros.		
CODIGO. **EC-159**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

1. Objetivo.

Establecer la metodología para el control de los documentos internos y externos que conforman el Sistema de Gestión de Seguridad de la Información, garantizando su adecuación, revisión, aprobación, actualización, legibilidad e identificación y prevención de obsolescencia.

2. Alcance.

Aplica a todos los documentos del SGSI, que se relacionen directamente con la comercialización y distribución de productos químicos.

3. Responsables.

Es responsabilidad del representante de la dirección para el SGSI, definir, controlar y hacer seguimiento a la documentación del Sistema.

4. Definiciones y Siglas.

- **Documento:** recopilación de datos que arrojan un significado, impresas en papel, medio magnético o sistematizado.
- **S.G.S.I:** Sistema de Gestión de Seguridad de la Información.
- **Documento Interno:** información o datos que posee y elabora la empresa a través de papel, disco magnético, óptico o electrónico y/o fotografías.

- **Documento Externo:** información o datos que poseen y elaboran organismos o personas ajenas a la empresa a través de papel, disco magnético, óptico o electrónico y/o fotografías. Este documento sirve de guía o apoyo para el desarrollo de las actividades.
- **Documento obsoleto:** son aquellos documentos que ya no tienen vigencia porque se han generado nuevas versiones mejoradas y que por lo tanto deben ser claramente identificados como tal en el SGSI.
- **Versión:** Muestra el estado de los documentos en términos de actualidad.

5. Metodología.

El control de los documentos es responsabilidad del representante de la dirección para el SGC, por medio del "Listado Maestro de Control de Documentos formato No. VAOMPC-RG02" donde se registra:

- Código del documento
- Nombre del Documento
- Si el Documento es Interno o Externo
- Versión
- Fecha de la última Revisión
- Responsable de la Revisión
- Responsable Aprobación
- Justificación del Cambio
- Distribución de Documentos (Control de original y copias)

CRITERIOS PARA CREACIÓN, MODIFICACIÓN Y/O ANULACIÓN DE DOCUMENTOS INTERNO Y EXTERNOS

1. La revisión realizada por parte de los jefes de procesos, a los cambios generados a procedimientos, instructivos y/o formatos contempla:

a. Revisión a la secuencia de actividades

b. Definición de responsable y documento por actividad

c. Codificación dada entre procedimientos, instructivos, formatos y los listados maestros de control de documentos y formatos.

Para tal efecto, quedará como evidencia la firma del jefe de proceso y la fecha de la revisión en el borrador respectivo.

2. Los cambios generados a los procedimientos y/o instructivos solo generarán nueva versión después de 5 modificaciones al mismo. De lo contrario serán informados a través del formato No. VAOMPC-RG14 Comunicaciones Reglamentarias de Procesos a todo el personal involucrado. Como control de esto el representante de la dirección para el SGSI, registrará la información en el formato "Manejo de Versión No. VAOMPC-RG05"

3. Todo documento externo que pueda afectar el sistema de calidad, debe ser entregado y revisado por del representante de la dirección del SGSI y el Jefe de Proceso antes de ser utilizado.

DIFUSIÓN CAMBIOS EN EL SISTEMA

1. Los cambios generados al sistema serán informados a través del formato No. VAOMPC-RG14 Comunicaciones Reglamentarias de Procesos por parte del representante de la dirección del SGSI.

2. El sistema se encuentra en las carpetas de cada una de las direcciones, adicionalmente, está en la página Web de la organización la cual solo sirve para consulta y tiene la opción de imprimir únicamente los formatos de cada proceso.

La metodología para el control de documentos se muestra en la siguiente matriz, donde se identifican las actividades, los responsables y los registros o documentos necesarios.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento de control de documentos.		
CODIGO. EC-159	ELABORADO. 20/01/2015	Versión. 01

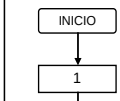
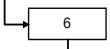
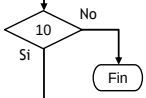
CONTROL DE DOCUMENTOS				
DIAGRAMA DE FLUJO	ACTIVIDAD	RESPONSABLE	DOCUMENTOS Y / O REGISTROS	
			CÓDIGO	NOMBRE
	Solicitar elaborar documento justificando su necesidad. (Se debe anexar modelo del documento)	Todos los empleados	VAOMPC-RG01	Solicitud de requerimiento a procesos
	Revisar la solicitud con el fin de asegurar su necesidad y validez. Entregar al representante del sistema según el proceso.	Jefe del Proceso	VAOMPC-RG01	Solicitud de requerimiento a procesos
	Aprobar los documentos con el fin de asegurar su necesidad y validez.	Representante del Sistema	VAOMPC-RG01	Solicitud de requerimiento a procesos
	El documento fue aprobado	Representante del Sistema	VAOMPC-RG01	Solicitud de requerimiento a procesos
	Informar a quien solicito el documento, que no fue aprobado y los motivos	Representante del Sistema		Mail
	Identificar el documento de acuerdo a la guía de elaboración de documentos y generarlo	Representante del Sistema	VAOMPC-IN01	Guía para la Elaboración de Documentos
	Revisar la documentación afectada con los cambios realizados	Jefe de Proceso		Documento con firma y fecha de la revisión.
	Informar a todo el personal involucrado sobre la existencia y los motivos del nuevo documento	Jefe del Proceso Representante del Sistema	VAOMPC-RG14	Comunicaciones reglamentarias a procesos Mail
	Asegurar la disponibilidad del documento en todos los sitios de trabajo	Representante del Sistema		Comunicado y actualización de carpetas, y pagina web
	El documento requiere de modificación y/o Anulación	Todos los empleados	VAOMPC-RG01	Solicitud de requerimiento a procesos
	Realizar todos los pasos a partir de la Actividad No. 2 hasta la No. 10			
	Identificar el documento que sale de vigencia con la palabra "obsoleto" y la fecha en que se da de baja.	Representante del Sistema		Documento con Sello de Obsoleto
	Fin del procedimiento			

Figura 42: Diagrama de Flujo del control de documentos.

Elaborado por: Autor.

6. Control de registros.

- **Registros en seguridad / organización y Métodos**

Tabla 33: Registros en seguridad/ organización y métodos.

CÓDIGO	NOMBRE DEL REGISTRO	ARCHIVO	ALMACENAMIENTO	PROTECCIÓN	RECUPERACIÓN		TIEMPO DE RETENCIÓN	
					QUIÉN	MÉTODO	RETENCIÓN	DIPOSICIÓN
VAOMPC-RG01	Solicitud de Requerimientos a Procesos	Físico	Archivador	AZ – Solicitud de requerimientos	Jefes de proceso	▪ Ordenado ascendentemente según fecha y número de la solicitud	1 año	Archivo Inactivo – Seguridad.
VAOMPC-RG14	Comunicaciones Reglamentarias de Procesos	Físico	Archivador	AZ Comunicados				
		Magnético	Computador - Mail	Clave – Back up mensual		▪ Carpeta comunicados SGSI.		
VAOMPC-RG05	Manejo de Versión	Magnético	Computador	Clave – Back up mensual		▪ c:\\mis documentos\carpeta registros		
VAOMPC-RG02	Listado Maestro de Control de Documentos	Físico	Escritorio	Fólder		• Ordenado ascendentemente según fecha de actualización		

Elaborado por: Autor.

- **Registros en las dependencias**

Tabla 34: Registros en las dependencias.

CÓDIGO	NOMBRE DEL REGISTRO	ARCHIVO	ALMACENAMIENTO	PROTECCIÓN	RECUPERACIÓN		TIEMPO DE RETENCIÓN	
					QUIÉN	MÉTODO	RETENCIÓN	DIPOSICIÓN
VAOMPC-RG14	Comunicaciones Reglamentarias de Procesos	Físico	Archivador	Fólder de Calidad Comunicados	Jefes de proceso	▪ Ordenada por mes y por número de radicación ▪ Ordenado ascendentemente	1 año	Archivo Inactivo - Calidad

Elaborado por: Autor.

ANEXO 5: AUDITORÍAS INTERNAS

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para auditorías internas.		
CODIGO. **EC-160**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

PROCEDIMIENTO PARA AUDITORÍAS INTERNAS.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para auditorías internas.		
CODIGO. **EC-160**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

1. Objetivo.

Determinar las responsabilidades y Requisitos para la Planificación y Realización de Auditorías, para informar de los resultados y para mantener los registros correspondientes.

2. Alcance.

Este Procedimiento es aplicable a las auditorías Internas que se realicen en el modelo de negocio dedicado a la comercialización y distribución de productos químicos.

3. Responsables.

El Coordinador de Sistema de Gestión de Seguridad de la Información es responsable de elaborar este procedimiento. El Gerente General es responsable de revisar y aprobar este procedimiento, que incluye la asignación del Auditor Líder.

El Auditor Líder es Responsable de:

1. Asistir a la elección del Equipo de Auditores Internos.
2. Preparar el Plan Anual y el Programa de cada Auditoria Interna.
3. Representar el Equipo frente a la Gerencia de la Organización (Conducción de Reuniones Iníciales, Final e Informativas).
4. Coordinar la actuación del Equipo Auditor.
5. Tomar las Decisiones Finales sobre la Auditoria y sus Hallazgos.
6. Presentar el Informe de Auditoria.

Todo el Personal tiene la responsabilidad de cumplir las disposiciones establecidas en este procedimiento.

4. Descripción de actividades.

4.1 Los Auditores.

El Auditor o Auditores tienen las siguientes responsabilidades:

- Clarificar a los auditores el motivo y circunstancias de la auditoría.
- Anotar todas las observaciones relevantes (evidencias objetivas) recogidas en el área auditada, y conservar copias de los documentos que las respalden.
- Ser objetivo y justo en sus apreciaciones.
- Colaborar con el auditor líder en todo lo necesario para asegurar el éxito de la auditoría.

Consecuentemente, los auditores deben reunir conocimientos técnicos suficientes sobre el área a auditar, y es preferible que tenga conocimientos específicos sobre las norma NTE INEN-ISO/IEC 27001:2011 aplicable, y también sobre auditorias. Actualmente esta tarea la puede desarrollar cualquier empresa certificada para realizar este tipo de procesos o cualquier persona que tenga personal a su cargo, y que previamente haya sido instruida en auditorias del Sistema de Gestión de Seguridad de la Información ISO 27001.

4.2 El Auditado.

Las responsabilidades del auditado son las siguientes:

- Poner a disposición del equipo auditor los medios necesarios para la auditoría.

- Facilitar el acceso a las instalaciones y documentos relevantes para la auditoría
- Cooperar con los auditores para asegurar el éxito de la auditoría.
- Poner en marcha las acciones correctivas que se deriven del informe de auditoría.

5. Desarrollo.

A partir del Plan Anual de Auditoría Internas, se procede de la siguiente manera:

I. Auditor Líder, elabora el plan anual de auditorías, considerando:

- Estado e importancia de los procesos y las áreas a auditar.
- Resultados de auditorías previas, cuando existan.

El plan de auditoría es flexible para permitir cambios en su alcance y extensión, así como para usar efectivamente los recursos.

II. El Gerente General, Revisa que el Plan de Auditorias es Conforme con las Disposiciones Planificadas, con los requisitos de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011, dependiendo del Objetivo de la Auditoria y con los Requisitos del Sistema de Gestión.

III. Auditor Líder, elabora el "Programa de Auditoría" para lo cual se debe considerar:

- Estado e importancia de los procesos
- Las áreas a auditar
- Resultado de auditorías previas

- Definir los criterios de auditoría
- Alcance dela auditoría
- Frecuencia y metodología
- Selección de auditores

IV. Auditor Líder, realiza reunión de apertura en la cual se presenta al equipo auditor y fija las reglas básicas para la efectiva realización de la auditoría. Como mínimo en la reunión de apertura se encontraran el equipo auditor, el representante de la dirección y representantes de las áreas auditadas. Registra la asistencia a esta reunión en el formato "Control de Asistencia" (Formato libre). En caso de ausencia de cualquiera de estos funcionarios, ellos mismos deberán designar su reemplazo. Revisa con los asistentes el objetivo, el alcance, los criterios a aplicar y la forma en que se va a ejecutar la auditoría.

V. Equipo de Auditores, realiza la auditoria según el programa elaborado.

VI. Auditores, reúnen evidencias objetivas a través de entrevistas, revisión de los documentos, registros y de la observación de los procesos y actividades.

VII. Equipo de Auditores, registra la no conformidad cuando se haya incumplido con los requisitos de seguridad. Registra en el formato "Reporte de No Conformidad y Acciones Correctivas", descripción de No Conformidad, el elemento de la norma que incumple, el área, la fecha y el auditor responsable.

VIII. Auditores/ Departamento de Seguridad de la Información, participan en la reunión de enlace, la que se realiza al final de cada auditoría para revisar las No Conformidades y observaciones que se han presentado durante el día.

IX. Auditor Líder, concluido el informe convoca a la reunión de cierre en la cual estarán presente el asistente de la reunión de apertura, en la medida de lo posible. En esta reunión se expresa un comentario general de la auditoría, se presentan los resultados comentando el "Informe de Auditoria" (Formato Libre). Registra la asistencia de los funcionarios a la reunión de cierre en el formato Control de Asistencia (Formato Libre).

X. Auditores, presentar en la reunión de cierre el total de las No Conformidades Levantada.

XI. Auditor Líder, entrega a los Gerentes o Jefes Departamentales y al Jefe del Departamento de Seguridad de la Información, las No Conformidades levantadas.

XII. Auditor Líder, elabora el informe de auditoría (Formato Libre), con copia para el Gerente General y Jefe del Departamento de Seguridad de la Información.

XIII. Jefe del Departamento de Seguridad de la Información, realiza el "Análisis de la Causa" y registra sus conclusiones en el "Reporte de No Conformidad y Acciones Correctivas". Tomar sin demora injustificada acciones para eliminar las No Conformidades detectadas y sus causas indicando la fecha máxima de

la implantación de esta acción. Las acciones deben ser apropiadas a los efectos de las No Conformidades encontradas.

XIV. Auditores, realiza el seguimiento de las acciones tomadas en la fecha posterior a la establecida como plazo y registra los resultados en el formulario "Reporte de No Conformidad y Acciones Correctivas".

XV. El Jefe del Departamento de Seguridad de la información, verifica acciones correctivas y firma reportes de No Conformidades. Si la acción correctiva no ha eliminado la causa de la No Conformidad, los responsables del área auditada debe volver a realizar el análisis de causas y tomar las acciones necesarias hasta que se elimine el origen del incumplimiento, la efectividad de las acciones correctivas, se realiza posterior a la fecha de seguimiento. Si la verificación es exitosa, firma el "Reporte de No Conformidad y Acciones Correctivas" como evidencia del cumplimiento y da por cerrada la No Conformidad.

6. Criterios de Auditoría.

Los criterios de auditoria aplicados son:

- Todos los elementos de la Norma NTE INEN-ISO/IEC 27001:2011, excluyendo solamente las excepciones consideradas en el alcance del S.G.S.I.
- Manual de Gestión de Seguridad de la Información.
- Normas, especificaciones y requisitos legales identificados por la organización.

Los incumplimientos detectados durante una auditoria, se los clasifican como:

No Conformidad Mayor. Se tiene este tipo de no conformidad en los siguientes casos:

- El incumplimiento total de una cláusula de la Norma (NTE-ISO/IEC 27001:2011).
- El incumplimiento total de lo señalado en los documentos de trabajo establecidos por la organización.
- El incumplimiento de un requisito legal.

No Conformidad Menor. Este tipo de no conformidad incluye todos aquellos incumplimientos detectados durante una auditoria y que no constituya ningún caso de no conformidad mayor. Por ejemplo: incoherentes entre la evidencia objetiva y lo declarado en los documentos, incumplimientos puntuales evidenciados en los registros requeridos por la norma o por el personal auditado.

7. Referencia.

Norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011

8. Registros.

a) Plan de auditoría

Tabla 35: Formato para Auditorías Internas.

Nombre de Compañía	
Tipo de Auditoría	
☐ Pre-Auditoría	Otros :
☐ Seguimiento	
Equipo Auditor	
Objetivos de Auditoría	• Auditar la documentación del sistema de gestión. • Evaluar la ubicación y las condiciones específicas del sitio e intercambiar información con el personal con el fin de determinar el estado de preparación para la auditoría de la etapa 2; • Proporcionar un enfoque para la planificación de la auditoría de la etapa 2, obteniendo una comprensión suficiente del sistema de gestión del cliente y de las operaciones del sitio en el contexto de los posibles aspectos significativos
Alcance de Auditoría	
Criterio de Auditoría & **Documentos de Referencia**	

Fuente: Autor.

b) Informe de Auditoría.

Informe de Auditoría interna realizada al del SGSI.

Objetivos de la auditoría

Los objetivos de esta auditoría son:

1. Verificar que el sistema de gestión de seguridad de la información de la organización cumple con los requisitos de las normas técnica NTE INEN-ISO/IEC 27001:2011.
2. Verificar que se estén cumpliendo todos los procedimientos y mecanismos de control que son demandados por la norma.

Resumen Auditoria

La auditoría se llevó a cabo los días 6, 7 y 8 de Enero de 2015, bajo el criterio de la norma técnica ecuatoriana NTE-INEN ISO/IEC 27001:2011.

Reunión de Inicio

La reunión inicial se desarrolló en la matriz de la organización. En ella se trató el procedimiento utilizado para la realización de la auditoría interna, los objetivo y alcance de la auditoría, la metodología de trabajo, la confidencialidad, el modo de clasificación de los hallazgos, y su tratamiento. Se confirmó el plan de auditoría enviado con anticipación.

Desarrollo de la Auditoría

El equipo auditor ha llevado a cabo un proceso de auditoría basado en los procesos de comercialización y distribución de productos químicos. Las fuentes de información revisadas incluyeron procedimientos, registros y entrevistas con el personal responsable de los diferentes procesos auditados.

Política, Objetivos y Programas

La política interna de la organización ha sido dada a conocer por medio de publicaciones a todo el personal interno. En relación a los objetivos, éstos se encuentran establecidos y dados a conocer a los cargos más altos de la organización.

Del análisis realizado en base al cumplimiento de los Objetivos y programas de gestión, se puede establecer que la el departamento de seguridad de la información presenta una mejora sustancial en el desempeño de los procesos monitoreados.

Documentación

La Organización ha desarrollado un Manual de Gestión de Seguridad de la Información, en el cual se define el cumplimiento de los requisitos establecidos por la norma técnica ecuatoriana INEN NTE-ISO/IEC 27001:2011.

La organización ha desarrollado manuales en los cuales se evidencia las políticas de seguridad, los procedimientos y mecanismos de control, así como la metodología de análisis y evaluación de riesgo.

Acciones Correctivas/preventivas

Se pudo evidenciar que la el departamento de seguridad de la información ha implementado las acciones necesarias para solucionar las no conformidades detectadas, pero estas no se han cerrado y/o no se ha establecido la eficacia de las mismas.

Resultados de la Auditoría

El resultado de esta auditoria se resume en el siguiente cuadro:

Tabla 36: Resultado de auditorías internas.

Nº de No Conformidades Mayores	0
Nº de No Conformidades Menores	5
Nº de Observaciones	2
Nº de Oportunidades de Mejora	1

Elaborado por: Autor.

Es recomendable que las observaciones detectadas se traten mediante el procedimiento de acciones preventivas, con la finalidad de evitar que éstas se conviertan en No Conformidades reales en una próxima auditoría.

Reunión de Cierre

La reunión de cierre de la auditoría se desarrolló en la oficina Matriz de la organización.

ANEXO 6: REVISIÓN POR LA DIRECCIÓN.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para la revisión por la dirección.		
CODIGO. **EC-161**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

PROCEDIMIENTO PARA LA REVISIÓN POR LA DIRECCIÓN.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para la revisión por la dirección.		
CODIGO. **EC-161**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

1. Objetivo.

Establecer los aspectos correspondientes para la revisión por la Dirección relacionados con la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información, aplicado a un modelo de negocio de comercialización y distribución de productos químicos.

2. Alcance.

El procedimiento aplica para la revisión que realiza por parte de la Dirección al Sistema de Gestión de Seguridad de la Información.

3. Definiciones/Abreviatura.

- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel la organización.
- **Revisión:** Actividad emprendida para asegurar la conveniencia, la adecuación y eficacia del tema objeto de la revisión, para alcanzar unos objetivos establecidos.

4. Contenido.

La alta Dirección tiene la responsabilidad y autoridad para asegurar que los procesos y procedimientos necesarios para el sistema de gestión de seguridad de la información se establezcan, implementen y mantengan.

La Alta Dirección con apoyo del Jefe de Seguridad de la Información revisa el Sistema de Gestión de Seguridad de la Información semestralmente (cada 6 meses) verificando el cumplimiento o avance en el periodo evaluado, de aquí se determinan no conformidades y se ejecutan las acciones correctivas necesarias para asegurar el mejoramiento del SGSI.

Los Comités para la Preservación de la Imparcialidad y Certificador se reúnen al menos una vez al año.

4.1 Información para la revisión por la dirección.

- Resultados de las auditorías internas y externas.
- Retroalimentación del Comité para garantizar la imparcialidad.
- Estado de las acciones preventivas y correctivas.
- Acciones de seguimiento, provenientes de revisiones por la Dirección previas.
- Cumplimiento de los objetivos y las políticas establecidas.
- Cambios que puedan afectar al Sistema de Gestión.
- Apelaciones y quejas.
- Legislación vigente que aplique al Sistema de Gestión de Seguridad de la Información.
- Registros contables y financieros.

Además de información que sea considerada pertinente para llevar a cabo la revisión.

4.2 Revisión por la dirección.

Para la revisión La Alta Dirección del Sistema de Gestión de Seguridad de la Información se apoya en el Formato brindado por el departamento de Seguridad de la Información, el cual contiene todos los numerales de la norma y en el cual se puede apreciar el avance sobre cada numeral.

En la revisión que realiza la Dirección:

- Se analizan los resultados obtenidos en las auditorías internas y externas, y las acciones a implementar según los resultados de las mismas.
- Se analiza la gestión del Comité para garantizar la imparcialidad.
- Se verifica el cumplimiento oportuno de las acciones correctivas y preventivas planteadas con anterioridad, y se registra el estado en el que se encontraron las mismas.
- Se realiza seguimiento al cumplimiento de las acciones definidas en anterior revisión realizada por la Dirección
- Se analiza el cumplimiento de los objetivos y las políticas establecidas según normatividad vigente.

- Se analizan cambios generados tanto al interior como al exterior del Organismo, con el fin de redefinir políticas y planeación ajustándose a las necesidades actuales.
- Se verifican las respuestas oportunas y las acciones derivadas de las quejas y apelaciones presentadas en el periodo.
- Se realiza análisis de los estados financieros y notas contables, con el fin de garantizar que el departamento de Seguridad de la Información dispone de estabilidad financiera y que cuenta con los recursos necesarios para el funcionamiento de su sistema de Gestión de Seguridad de la Información.
- Se revisan los procesos que se desarrollan en el departamento de Seguridad de la Información, con el fin de verificar que se encuentran funcionado de acuerdo a lo establecido.
- Se verifica que todo el personal se encuentre dando cumplimiento a las funciones que le han sido asignadas, lo cual debe constituirse en un insumo para la evaluación del desempeño.
- La Alta Dirección realiza seguimiento a los objetivos de seguridad de la información dentro de la organización con el fin de evaluar el cumplimiento de las metas establecidas y la obtención de resultados.

4.3 Resultados de la revisión por parte de dirección.

Los resultados de la revisión determinan decisiones y acciones referentes a la mejora de la eficacia del Sistema de Gestión de Seguridad de la Información y de los procesos.

Estos resultados son comunicados a todos los integrantes del Organismo.

La Alta Dirección presenta al Comité para la Preservación de la Imparcialidad los resultados de las revisiones realizadas. Dicho informe de resultado debe incluir el Plan de acción que desarrolla con el fin de mejorar las no conformidades encontradas en cada uno de los casos analizados. De la reunión con el Comité se realiza acta.

El Plan de Acción es revisado en las sesiones y de acuerdo a las fechas establecidas se hace un informe del cumplimiento de las mejoras evidenciándolas.

Los resultados de la revisión de la Dirección se dan a conocer a todo el personal del departamento de Seguridad de la Información.

La Alta Dirección verifica y evalúa el estado del Organismo, haciendo un seguimiento a la eficacia, para ello utiliza un documento de seguimiento.

5. Responsabilidades.

Tabla 37: Responsabilidades del procedimiento de revisión por la dirección.

RESPONSABLE	RESPONSABILIDADES
Director	• Realizar revisión anual del SGSI. • Implementar, actualizar y divulgar el procedimiento. • Custodiar la documentación que está a su cargo. • Comunicar a los integrantes los resultados de la revisión de la Dirección.
RESPONSABLE	**RESPONSABILIDADES**
Jefe de Seguridad de la Información.	• Custodiar la documentación que está a su cargo. • Apoyar la revisión del SGSI. • Realizar preparativos logísticos para la revisión. • Convocar a los comités a las reuniones. • Generar acta de las revisiones, realizar seguimiento a acuerdos.
Comité para la Preservación de la Imparcialidad.	• Asesorar en la toma de decisiones relacionada con el SGSI. • Realizar seguimiento al SGSI. • Realizar seguimiento a quejas, apelaciones, acciones correctivas y acciones preventivas. • Verificar el estado de las auditorías internas y externas.

Funcionarios.	• Revisar el Sistema de Gestión en lo correspondiente a sus funciones. • Realizar mejoras. • Facilitar la información requerida por la Dirección.

Elaborado por: Autor.

ANEXO 7: ACCIONES CORRECTIVAS Y PREVENTIVAS.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para las acciones correctivas y preventivas.		
CODIGO. **EC-163**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

PROCEDIMIENTO PARA LAS ACCIONES CORRECTIVAS Y PREVENTIVAS.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para las acciones correctivas y preventivas.		
CODIGO. **EC-163**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

1. Objetivo.

Establecer los procedimientos para la ejecución de las acciones correctivas y preventivas, con la finalidad de eliminar las causas que originan no conformidades que afectan al Sistema de Gestión de Seguridad de la Información.

2. Alcance.

El procedimiento hace referencia a los requerimientos 8.3 (Acciones Correctivas) y 8.4 (Acciones Preventivas) de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011.

El procedimiento se aplica al personal involucrado en llevar a cabo las acciones correctivas y hacer cumplir lo establecido como una solución para eliminar las causas que originaron la No Conformidad.

3. Definiciones/Abreviatura.

- **Acción Correctiva:** Acción tomada para eliminar las causas de una no conformidad detectada y otra situación indeseable.
- **Acción Preventiva:** Acción tomada para eliminar la causa de una no conformidad potencial y otra situación potencialmente indeseable.

4. Descripción del procedimiento.

4.1 Acciones Correctivas.

- Las acciones correctivas son iniciadas, controladas y documentadas por medio del uso del formulario No Conformidad, Acción Correctiva y Preventiva
- Los orígenes de las acciones correctivas pueden venir de diversas fuentes, tales como:
    - No conformidades.
    - Auditorías internas.
    - Auditorías externas.
    - Eventos de seguridad.
    - Otros orígenes.
- El Encargado del Sistema de Gestión de Seguridad de la Información deberá analizar cada una de las No Conformidades y derivara la no conformidad al área correspondiente (Director/Jefatura), la cual asignará al personal que identificar a la causa raíz del problema.
- A través del formulario No Conformidad, Acción Correctiva y Preventiva, se registrará la causa raíz y la acción correctiva propuesta para proceder a implementarla.

- Una vez implementada la acción correctiva el encargado del Sistema Gestión de Seguridad de la Información verificará que el problema haya sido efectivamente solucionado, y firmará el formulario en el área señalada para tal efecto.
- En el caso que la no conformidad no sea resuelta, volverá analizar el problema para encontrar la acción correctiva más apropiada, según lo indicado en el punto anterior.
- El Encargado del Sistema de Gestión de Seguridad de la Información mantendrá los registros de las acciones correctivas cerradas y monitoreará las acciones que aún no han sido implementadas

4.2 Acciones Preventivas.

- Las acciones preventivas son iniciadas, controladas y documentadas por medio del uso del formulario No Conformidad, Acción Correctiva y Preventiva.
- Las acciones preventivas pueden surgir de las siguientes situaciones:
    - Para resolver debilidades o vulnerabilidades identificadas durante auditorías internas y externas.
    - Eliminar posibles no conformidades causadas por falta de procedimientos de seguridad.

- El Encargado del Sistema de Gestión de Seguridad de la Información deberá analizar o asignará al personal para identificar las potenciales no conformidades y derivara la no conformidad potencial al área correspondiente (Director/Jefatura), la cual deberá determinar las acciones preventivas que ameriten ser implementadas.
- A través del formulario No Conformidad, Acción Correctiva y Preventiva, Se registrará la acción preventiva propuesta, para proceder a implementarla.
- Una vez implementada la acción preventiva el encargado del Sistema de Gestión de Seguridad de la Información verificará que el potencial problema haya sido efectivamente solucionado, y firmará el formulario en el área señalada para tal efecto.
- El Encargado del Sistema de Gestión de Seguridad de la Información mantendrá los registros de las acciones preventivas cerradas y monitoreará las acciones que aún no han sido implementadas.

5. Responsabilidades.

La responsabilidad por el cumplimiento del procedimiento recae sobre el Jefe de Seguridad de la Información o sobre el Oficial de Seguridad de la Información.

6. Registros.

Registro para acciones correctivas y preventivas.

Tabla 38: Registro de acciones correctivas y preventivas.

Nombre de compañía					
Sitio					
Mayor	**Menor**	**Proceso / Procedimiento**			
Hallazgo					
Firma de Auditor líder		**Firma de Representante de la Dirección**		**Fecha acordada para el cierre**	
Análisis de Causa Fundamental (diligenciado por la compañía)					
Corrección (diligenciado por la compañía)					
Firma de Representante de la Dirección			**Fecha del Cierre**		
Verificación de Corrección					
Satisfactoria?		**Comentarios**			
SÍ __	**NO __**				
Acción Correctiva (diligenciado por la compañía)					
Firma de Representante			**Fecha del Cierre**		
Verificación de Acción Correctiva					
Satisfactoria?		**Comentarios:**			
SÍ __	**NO __**				
Firma de Auditor				**Fecha**	

Elaborado por: Autor.

ANEXO 8: ANÁLISIS Y EVALUACIÓN DE RIESGOS.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para el análisis y evaluación de riesgos.		
CODIGO. **EC-180**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

PROCEDIMIENTO PARA EL ANÁLISIS Y EVALUACIÓN DE RIESGOS.

ENERO DEL 2015.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Procedimiento para el análisis y evaluación de riesgos.		
CODIGO. **EC-180**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

1. Objetivo.

Establecer los procedimientos para en análisis y evaluación de riesgos, con el objetivo de evaluar los riesgos mediante el proceso dirigido a estimar la magnitud de los mismos, que no hayan podido evitarse mediante su identificación análisis, evaluación y registro.

2. Alcance.

El procedimiento es aplicado a todas las áreas que se encuentren involucradas en la comercialización y distribución de productos químicos.

3. Definiciones/Abreviatura.

- **Riesgo:** Combinación de la frecuencia o probabilidad que puedan derivarse de la materialización de un peligro.
- **Análisis de Riesgo:** Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- **Estimación de Riesgo:** El proceso mediante el cual se determina la frecuencia o probabilidad y las consecuencias que puedan derivarse de la materialización de un peligro.
- **Evaluación de riesgos:** El proceso general de análisis y estimación de los riesgos.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

4. Descripción del procedimiento.

4.1 Metodología de Análisis de Riesgos.

El análisis, la cuantificación y gestión del riesgo de las operaciones aplicadas a una organización con un modelo de negocio enfocado a la distribución y comercialización de productos químicos, ha sido desarrollado acorde a la metodología de gestión de riesgos MAGERIT.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), busca un método aproximado para el análisis de riesgos y para la gestión de seguridad.

4.2 Metodología de Análisis de Riesgos.

El análisis, la cuantificación y gestión del riesgo de las operaciones aplicadas a una organización con un modelo de negocio enfocado a la distribución y comercialización de productos químicos, ha sido desarrollado acorde a la metodología de gestión de riesgos MAGERIT.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), busca un método aproximado para el análisis de riesgos y para la gestión de seguridad.

4.3 Análisis y evaluación del riesgo.

Mediante la utilización de la metodología de MAGERIT se expone la siguiente estructura para el correcto análisis de riesgo de una industria química.

En la realización de un Análisis y Gestión de Riesgos según el Ministerio de Hacienda y Administraciones Públicas de España (2012), en su ponente ilustración MAGERIT – versión 3.0, indica que "el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos", los cuales se detallan a continuación.

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

- El sistema de información propiamente dicho del Dominio (hardware, redes, software, aplicaciones)
- La propia información requerida, soportada o producida por el Sistema de Información que incluye los datos informatizados, así como su estructuración (formatos, códigos, claves de cifrado) y sus soportes (tratables informáticamente o no)
- Las funcionalidades del Dominio que justifican al Sistema de Información, incluido desde el personal usuario a los objetivos propuestos por la dirección del Dominio.

- Otros Activos, de naturaleza muy variada, por ejemplo la imagen de la organización, la confianza que inspire, el fondo de comercio, la intimidad de las personas, etc.

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

- **Desastres naturales:** Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
- **De origen industrial:** Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
- **Errores y fallos no intencionados:** Fallos no intencionales causados por las personas.
- **Ataques intencionados:** Fallos deliberados causados por las personas.

Las Amenazas se encuentran clasificadas de la siguiente manera.

Grupo A de Accidentes

- A1: Accidente físico de origen industrial: incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radioeléctricas

- A2: Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema
- A3: Accidente físico de origen natural: riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe
- A4: Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos y suministros diversos
- A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática.

Grupo E de Errores

- E1: Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema
- E2: Errores de diseño existentes desde los procesos de desarrollo del software (incluidos los de dimensionamiento, por la posible saturación)
- E3: Errores de ruta, secuencia o entrega de la información en tránsito
- E4: Inadecuación de monitorización, trazabilidad, registro del tráfico de información

Grupo P de Amenazas Intencionales Presenciales

- P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura)

- P2: Acceso lógico no autorizado con intercepción pasiva simple de la información
- P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración; es decir, reducción de la confidencialidad para obtener bienes o servicios aprovechables (programas, datos)
- P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración: es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica)
- P5: Indisponibilidad de recursos, sean humanos (huelga, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo).

Grupo T de Amenazas Intencionales Tele-actuadas

- T1: Acceso lógico no autorizado con intercepción pasiva (para análisis de tráfico)
- T2: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración
- T3: Acceso lógico no autorizado con modificación (Inserción, Repetición) de información en tránsito

- T4: Suplantación de Origen (del emisor o reemisor, ‘man in the middle’) o de Identidad

Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

Tabla 39: Ocurrencias de vulnerabilidad.

Promedio medio entre ocurrencias	Escala subjetiva
Menor de 1 semana	Frecuencia muy alta
Menor de 2 meses	Frecuencia alta
Menor de 1 año	Frecuencia media
Menor de 6 años	Frecuencia baja
Superior a 6 años	Frecuencia muy baja

Elaborado por: Autor.

Impactos: Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto

- N1: Pérdidas de valor económico, ligadas a activos inmobiliarios o inventaríales (costes de reposición de la funcionalidad, gastos de tasar, sustituir, reparar o limpiar lo dañado, edificios y obras, instalaciones, computadores, redes)
- N2: Pérdidas indirectas, valorables y ligadas a intangibles en general no inventariados (datos, programas, documentación, procedimientos)
- N3: Pérdidas indirectas, valorables económicamente, unidas a disfuncionalidades tangibles (coste del retraso o interrupción de funciones operacionales de la organización; la perturbación o ruptura

de los flujos y ciclos productivos, incluido el deterioro de la calidad de éstos; y la incapacidad de cumplimentar las obligaciones contractuales o estatutarias)

- N4: Pérdidas económicas relativas a responsabilidad legal del 'propietario' del Dominio protegible siniestrado debido a los perjuicios causados a terceros (multas)

Otros deterioros de los sub-estados de seguridad tienen Impactos con consecuencias cualitativas orgánicas de varios tipos:

- L1: Pérdida de fondos patrimoniales intangibles: conocimientos (documentos, datos o programas) no recuperables, información confidencial
- L2: Responsabilidad penal por Incumplimiento de obligaciones
- L3: Perturbación o situación embarazosa político-administrativa (credibilidad, prestigio, competencia política)
- L4: Daño a las personas

5. Responsabilidades.

La responsabilidad por el cumplimiento del procedimiento recae sobre el Jefe de Seguridad de la Información o sobre el Oficial de Seguridad de la Información.

ANEXO 9: MATRIZ DE ANÁLISIS Y EVALUACIÓN DE RIESGOS.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Matriz de Análisis y Evaluación de Riesgos.		
CODIGO. **EC-200**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

MATRIZ DE ANÁLISIS Y EVALUACIÓN DE RIESGOS.

ENERO DEL 2015.

ELABORO: Xavier Aguila	REVISO:	APROBO:
FECHA: 20/01/2015	FECHA:	FECHA
Subsistema de Gestión de Seguridad de la Información (SGSI)		
Matriz de Análisis y Evaluación de Riesgos.		
CODIGO. EC-200	**ELABORADO. 20/01/2015**	**Versión. 01**

Tabla de Contenido.

ELABORO: Xavier Aguila	REVISO:	APROBO:
FECHA: 20/01/2015	FECHA:	FECHA:
Subsistema de Gestión de Seguridad de la Información (SGSI)		
Matriz de Análisis y Evaluación de Riesgos.		
CODIGO. EC-200	**ELABORADO. 20/01/2015**	**Versión. 01**

i) Objetivo.

A través de este documento se expresa formalmente las decisiones de la Gerencia del Proyecto SI, con relación al análisis y diagnóstico de riesgos dentro de la organización como lo indica la norma técnica NTE INEN-ISO/IEC 27001:2011, realizado en el marco del establecimiento del Sistema de Gestión de Seguridad de la Información.

ii) Indicadores.

Como parámetros para el establecimiento de calificación acorde al tipo de riesgo que se tiene expuesto, se proponen los siguientes indicadores.

Tabla 40: Tabla de indicadores para la estimación de riesgos.

Probabilidad.	Impacto	Producto	Nivel de Riesgo.	Resultado.	Tratamiento.	
1	5	5	8%	Bajo	Aceptable	Asumir el riesgo. Permite a la Empresa asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.
1	10	10	17%	Bajo	Tolerable 1	Asumir o reducir el riesgo. se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible.

2	5	10	17%	Bajo	Tolerable 2	Asumir o reducir el riesgo. se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. Cuando la Probabilidad del riesgo es media y su Impacto leve, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo.
3	5	15	25%	Medio	Moderado 1	Evitar el riesgo, se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. los Riesgos de Impacto leve y Probabilidad alta se previenen.
2	10	20	33%	Medio	Moderado 2	Reducir, Evitar, Compartir o transferir el riesgo. se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. los Riesgos con Impacto moderado y Probabilidad media, se reduce o se comparte el riesgo, si es posible.
1	20	20	33%	Medio	Moderado 3	Reducir, Compartir o transferir el riesgo. Cuando el riesgo tiene una Probabilidad baja e Impacto catastrófico se debe tratar de compartir el riesgo y evitar la Empresa en caso de que éste se presente. Siempre que el riesgo es calificado con Impacto catastrófico la Empresa debe

						diseñar planes de contingencia, para protegerse en caso de su ocurrencia.

Subsistema de Gestión de Seguridad de la Información (SGSI)		
Matriz de Análisis y Evaluación de Riesgos.		
CODIGO. **EC-200**	**ELABORADO.** **20/01/2015**	**Versión.** **01**

3	10	30	50%	Alto	Importante 1	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico
2	20	40	67%	Alto	Importante 2	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. Es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. El riesgo es calificado con Impacto catastrófico la Empresa debe diseñar planes de contingencia.
3	20	60	100%	Alto	Inaceptable	Evitar, Reducir, Compartir o transferir el riesgo. Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Probabilidad del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles. Siempre que el riesgo sea calificado con Impacto

						catastrófico la Empresa debe diseñar planes de contingencia.

Fuente: Tomado del libro de MAGERIT.
Elaborado por: Autor.

iii) Matriz de Riesgo.

Después de haber logrado evidenciar las posibles vulnerabilidades que afectan la seguridad de la información, se expone la siguiente matriz de riesgo aprobada y revisas por la dirección.

Tabla 41: Matriz de riesgo.

N	Objetivo de Control.	Calificación preliminar de Probabilidad.	Calificación preliminar de Impacto.	Evaluación Preliminar de Riesgo.	Control Propuesto.	¿Disminuye el nivel de probabilidad del riesgo?	¿Disminuye el nivel de impacto del riesgo?	Valoración Probabilidad	Valoración Impacto	Valoración riesgo	Opciones manejo
1	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO A.9.1.2 Controles de acceso físico. Control Las áreas seguras deben estar protegidas con controles de acceso	3	20	Inaceptable	Establecer un área segura con controles de acceso y apertura de puerta electrónica	Si	Si	2	20	Importante 2	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. Siempre que el

	apropiados para asegurar que sólo se permite el acceso a personal autorizado.				con acceso biométrico						riesgo es calificado con Impacto catastrófico la Empresa debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.
2	A.9.2.3 Seguridad del cableado. Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.	2	10	Moderado 2	Establecer un área segura con controles de acceso y apertura de puerta electrónica con acceso biométrico	Si	No	1	10	Tolerable 1	Asumir o reducir el riesgo. se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible.
3	A.9.2.6 Seguridad en la reutilización o eliminación de los equipos. Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos	2	10	Moderado 2	Establecer un procedimiento de reutilización o eliminación de los equipos de cómputo, donde se utilice una herramienta de	Si	Si	1	5	Aceptable.	Asumir el riesgo. Permite a la Empresa asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

					borrado a bajo nivel de los datos contenidos en el disco duro.						
4		1	5	Aceptable		si	no	1	5	Aceptable	Asumir el riesgo. Permite a la Empresa asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Elaborado por: Autor.

ELABORO: Xavier Aguila	**REVISO:**	**APROBO:**
FECHA: 20/01/2015	**FECHA:**	**FECHA**

ANEXO 10: FORMATO DE ENCUESTAS REALIZADAS.

Estimado Ing., de manera muy cordial se lo invita a responder el siguiente cuestionario, estas preguntas tienen el objetivo de recolectar su importante opinión referente a la importancia de un Sistema de Gestión de la Seguridad de la Información, en las organizaciones con un modelo de negocio dedicado a la comercialización y distribución de productos químicos. Ésta información ayudará a darle validez y a indicar que este proyecto es viable, por tal razón es muy importante que sus respuestas sean honestas. Agradezco su participación.

Por favor marcar con una X su respuesta.

a) Sexo: Hombre ( ) Mujer ( )

b) Nombre:

c) Empresa:

1. ¿Considera usted que la información es el activo más crítico que puede tener la organización?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

2. ¿Considera usted que al diseñar un Sistema de Gestión de Seguridad de la información va a ayudar a gestionar la información y los recursos informáticos de manera óptima y segura?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

3. ¿Considera usted que al diseñar de manera correcta un Sistema de Gestión de Seguridad de la información va a brindar un reconocimiento corporativo en el mercado?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

4. ¿Considera que aplicando el criterio de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001:2011 va a garantizar los niveles de integridad, confidencialidad y disponibilidad de la información?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

5. ¿Cree usted que por medio de políticas de seguridad posible garantizar la seguridad de la información acorde a los requisitos del negocio?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

6. ¿Considera usted que los procedimientos y mecanismos de control aseguran que los procesos de seguridad de la información se realicen de manera segura?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

7. ¿Considera usted que una metodología de análisis de riesgo va a ayudar de gran manera a identificar y mitigar los posibles riesgos que existan dentro de su organización?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

8. ¿Considera usted que por medio de la evaluación de riesgos va a ser posible mitigar la mayor cantidad de vulnerabilidades existentes?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

9. ¿Considera usted que los controles informáticos enunciados son necesarios para las organizaciones?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )

10. ¿Cree usted que es necesario que la organización efectúe el análisis y diseño de un SGSI, para preservar los activos informáticos?

- Totalmente en desacuerdo ( )
- En desacuerdo ( )
- Ni de acuerdo ni en desacuerdo ( )
- De acuerdo ( )
- Totalmente de acuerdo ( )