UNIVERSIDAD DEL AZUAY

FACULTAD DE: CIENCIAS DE LA ADMINISTRACION

ESCUELA DE: INGENIERIA DE SISTEMAS Y TELEMATICA

PLAN DE GESTIÓN DE RIESGOS PARA MADECO CÍA. LTDA.

TESIS PREVIO A LA OBTENCIÓN DE TÍTULO DE:

INGENIERA DE SISTEMAS Y TELEMÁTICA

AUTOR: FERNANDA NIVICELA

DIRECTOR: ING. ESTEBAN CRESPO MBA

CUENCA, ECUADOR

2014

Dedicatoria

Este trabajo va dedicado a mis padres y hermanos que siempre estuvieron presentes apoyándome y dándome ánimo para seguir adelante. A ellos les debo haber alcanzado mis logros y metas. A través de su amor, su comprensión, supieron enseñarme siempre a ser perseverante y aprender de mis errores sin importar la magnitud de la dificultad o de los errores.

A mis primos-hermanos Silvia, Paulino, Patricia, Adriana, Santiago, aquellos con los que crecí, aquellos a los que siempre admiré y por los que siempre guardare respeto y mi eterna admiración. Con sus consejos, paciencia y a veces hasta cuando a pesar de las circunstancias hacían de profesores para poder enseñarme lo que necesitaba.

A mis amigos-compañeros que estuvieron conmigo en las buenas y en las malas, y que a pesar de las dificultades que se nos presentaban siempre salíamos adelante como un equipo. Compartimos tantas experiencias, emociones, triunfos y derrotas, pero siempre estábamos allí superando los obstáculos a pesar de la adversidad.

Agradecimiento

A mis profesores y amigos Ing. Juan Pablo Esquivel, Ing. Esteban Crespo M, Ing. Marcos Orellana por haberme guiado y aconsejado para la selección de mi tesis.

A la alta Dirección MADECO Cía. Ltda., por haberme permitido realizar un Plan de Gestión de Riesgos de la Información para su empresa y por la colaboración de todo el personal que me confió su información con el fin de desarrollar el presente trabajo de graduación.

Índice de Contenidos

Indice Ilustraciones y cuadros

Indice Anexos

Resumen

Este documento propone plantear la solución a un problema muy común en la actualidad, como es la falta de un Plan de Gestión de Riesgos en las PYME por falta de culturización y la idea errada de que las Tecnologías de Información son el último eslabón de la cadena operativa de la organización. Este es el caso de MADECO Cía., Ltda., una PYME cuencana con varios años en el mercado, dedicada a la distribución y comercialización de materiales de construcción, para la que se creará un Plan de Gestión de Riesgos basado en la ISO 27001:2005.

ABSTACT

This document proposes to find the solution to a very common current problem, as is the lack of a Risk Management Plan in SMEs (SMALL AND MEDIUM ENTERPRISES) due to lack of education and the mistaken idea that the Information Technologies are the last link in the operational chain of an organization. This is the case of MADECO Co., Ltd., a small business from Cuenca with several years in the market, dedicated to the distribution and marketing of building materials, for which a Risk Management Plan based on the ISO 27001: 2005 will be created.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,
Lic. Lourdes Crespo

Introducción

A lo largo de este documento se propone plantear la solución a un problema muy común en estos días, como es la falta de un Plan de Gestión de Riesgos que las PYME’s no disponen por la falta de culturización al respecto y la idea errada de que las Tecnologías de Información son el último eslabón de la cadena operativa de la organización. Este es el caso de MADECO Cía., Ltda., una PYME cuencana con varios años en el mercado, dedicada a la distribución y comercialización de materiales de construcción, empresa que no dispone de un Sistema de Gestión de Seguridad de la Información.

Crear un plan de gestión de riesgos de la información basada en la norma ISO 27001:2005, acorde a los controles y directrices que propone esta norma para la empresa Madeco Cía. Ltda.

Realizar un levantamiento de activos de información de la empresa MADECO Cía. Ltda.

Analizar y clasificar los activos de la información en una jerarquía tal que denote la importancia que juega cada uno con respecto a la misión de la empresa

Identificar y analizar todas las amenazas posibles, su grado de impacto y el nivel de ocurrencia con el que se puedan suscitar.

Identificar y analizar las vulnerabilidades que pueden ser explotadas por las amenazas y convertirse en riesgos para la empresa

Generar un plan de seguridad para cumplir con los controles (ISO 27001:2005).

CAPÍTULO 1: MARCO TEÓRICO

1.1. Introducción a la seguridad de la información

Actualmente debido a la globalización y al crecimiento continuo del comercio las empresas se han visto obligadas a ser cada vez más competitivas e innovadoras. Y es debido a ello que estas empresas realizan fuertes inversiones en la capacitación del personal para fomentar su creatividad y con ello lograr que los empleados innoven y materialicen sus ideas en productos, los que posteriormente son lanzados al mercado.

Se tiene varios ejemplos de innovación en Ecuador como por ejemplo EASA (Embotelladora Azuaya S.A. Líder en producción de bebidas espirituosas), Pronaca, Cervecería Nacional, Supermaxi, GRAIMAN, entre otras. Cada una de ellas resalta en cada uno de sus ámbitos gracias a la creatividad de su departamento de investigación y mercadeo. Pero ni las mejores características mencionadas son suficientes para asegurar que sus prototipos salgan al mercado antes que la competencia. Muchas de las veces pueden ser porque hay empresas más innovadoras y competitivas, pero en ciertos casos se pueden dar fugas de información, maquiladas por gente inescrupulosa.

A razón de este escenario nace la gestión de seguridad de la información, cuyo propósito es velar por la integridad, confidencialidad, y disponibilidad de la información, la cual muchas veces puede ser accedida por personas no autorizadas si no se establecen políticas y procedimientos adecuados para su control. Es por ello que para poder cumplir estos objetivos, se requieren de planes técnicos a nivel lógico y físico, legales reglamentarios, humanos y organizativos, puesto que cada uno de estos factores conforman un aspecto muy importante para el funcionamiento de la organización.

La implementación de un SGSI se logra a través de una serie de procesos, desde la planificación, hasta la monitorización y mejora continua. Los requerimientos iniciales para implementar un sistema de gestión de seguridad son: realizar un proceso de reconocimiento de activos que califican como esenciales para la estrategia de negocio, posteriormente analizar y evaluar los activos para finalmente ejecutar la gestión de riesgos necesaria para minimizar las amenazas que puedan impactar negativamente en la organización.

Un sistema de gestión de seguridad de la información se puede definir como el establecimiento de parámetros que determinan qué, por qué y cómo debe ser protegida la información valiosa de una empresa, para que mantenga su confidencialidad, integridad y disponibilidad definidos a continuación.

Integridad: Es la consistencia de la información. Los datos no pueden ser accedidos ni modificados por personas no autorizadas.

Confidencialidad: Prevención de divulgación de información a personas y sistemas no autorizados.

Disponibilidad: La capacidad de la información de estar disponible para su revisión por parte del personal que lo requiera.

Para poder asegurar la fiabilidad de este sistema se recomienda la aplicación de la defensa en profundidad, el cual consiste en manejar la seguridad a través de capas para reducir el riesgo de que atacantes externos o internos accedan fácilmente a información valiosa. Tales capas encapsulan recursos críticos en cada nivel como encriptación, gestión de usuarios, etc. (Alan Calder)

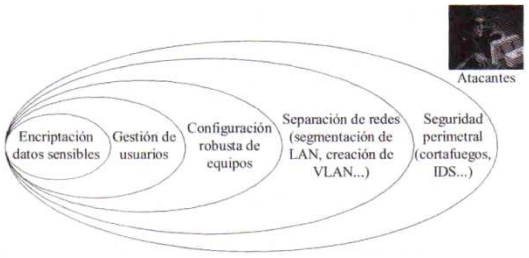


Gráfico 1: Defensa en profundidad (A. Gomez)

1.2. ISO 27001

Es un estándar Británico aprobado y certificable internacionalmente que proporciona un modelo para establecer, implementar, Gestiónar, mantener, y mejorar un Sistema de Gestión de Seguridad de la Información. Es aplicable a empresas de cualquier tamaño e índole, ajustable a los requisitos de seguridad que necesite la organización. La norma está diseñada bajo un enfoque dirigido a procesos. Para el desarrollo de este modelo se utilizan los insumos proporcionados por dueños, usuarios y administradores del sistema de la organización.

Este estándar tiene como pilares fundamentales los siguientes controles:

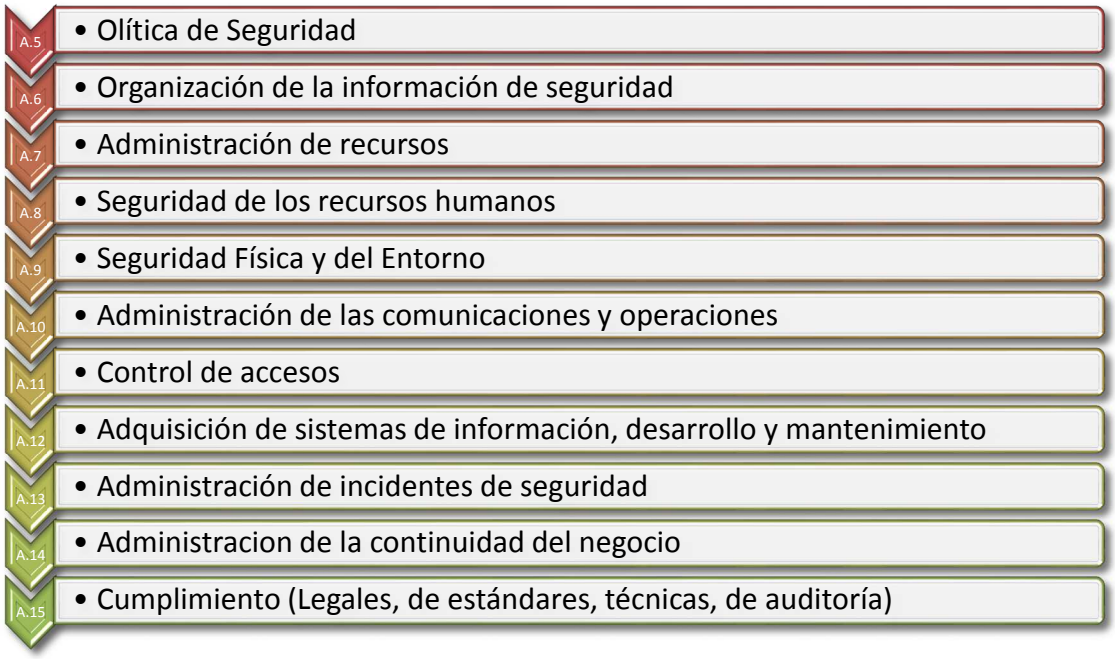


Tabla 1: Controles ISO 27001:2005 (Alberto G. Alexander, Diseño de un SGSI 25)

Sin embargo la norma no es estrictamente rígida con respecto al incremento de políticas y procedimientos propios para la empresa, si se desea se puede implementar nuevos controles que satisfagan sus consideraciones estratégicas particulares (objetivos, políticas).

El modelo de esta norma se basa en el ciclo PDCA: Plan, Do, Check, Act cuyo objetivo es el de reducir la posibilidad de que los activos de información sean afectados por amenazas internas o externas. Así mismo el presente modelo se basa en requerimientos o cláusulas globales y focales, los mismos que se encuentran distribuidos dentro del siguiente proceso:

Gráfico 2: Ciclo Deming. (PDCA) (A. Gomez)

Descripción de cláusulas focales:

Plan (Planear): Proceso durante el cual se establece el alcance del SGSI, el reconocimiento de procesos, levantamiento, análisis, tasación y evaluación de riesgos de los activos.

Do (Hacer): Periodo de implementación del SGSI, durante esta fase se determina un plan de tratamiento de riesgos en el cual se establecen los procedimientos a seguir para mitigar, disminuir o transferir los riesgos.

Check (Chequear): Utilizar métricas para evaluar el desempeño del SGSI dentro de la empresa.

Act (Actuar): Fase de mejora continua, se debe tomar medidas correctivas según el plan de gestión de continuidad de negocio.

Clausulas Globales:

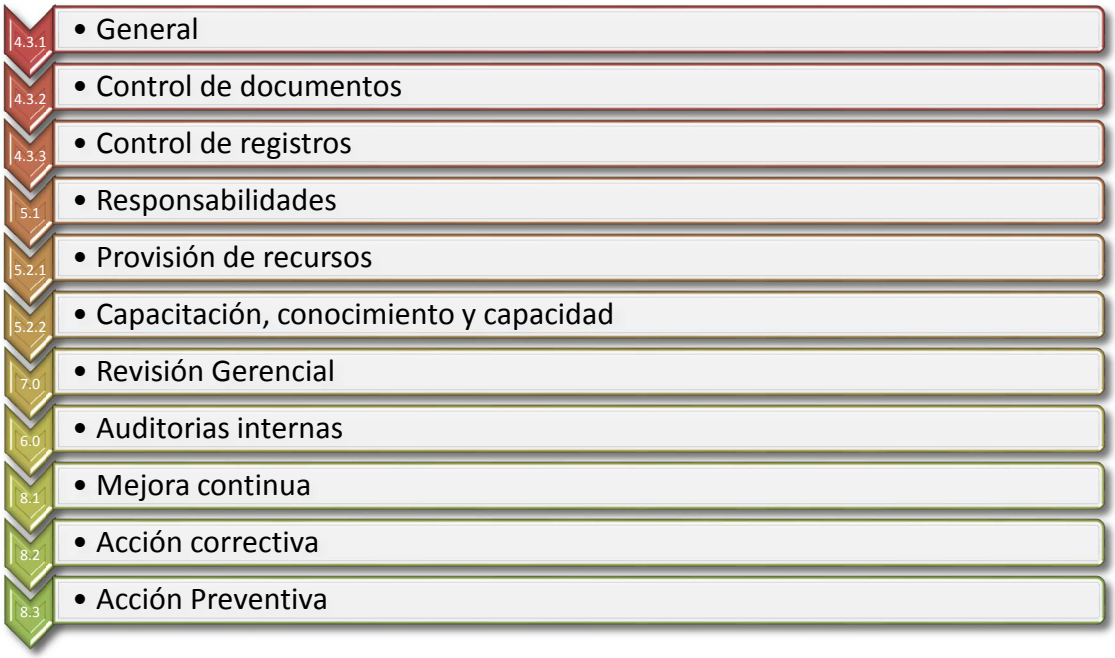


Tabla 2: Clausulas Globales
http://sites.amarillasinternet.com/brigadanacionaldebomberos/productos_servicios.html enero 22 de 2013

Las clausulas globales son de especial importancia, por lo que se deben documentar antes que las clausulas focales. A continuación se presentan la estructura de las clausulas globales.

La cláusula 4.3.1 de la norma ISO 27001:2005 establece que se debe llevar la documentación de las políticas, procedimientos y objetivos de control, así como el alcance del SGSI, el plan de tratamiento de riesgos, declaración de aplicabilidad, reportes de evaluación de riesgo y la descripción de la metodología de evaluación de riesgos. Cada uno de estos documentos debe tener datos importantes como fecha de emisión, firma de aprobación, prueba de que han sido revisados y que se haya controlado la modificación.

La cláusula 4.3.2 de la norma ISO 27001:2005 sobre control de documentos estipula que el responsable de la gerencia debe encargarse de la aprobación de documentos

previos a su emisión, revisarlos y actualizarlos, así como el control y registro de cambios de documentos, también de verificar la disponibilidad, legibilidad como la facilidad de identificación de documentos actuales. Validar que los documentos sean usados debidamente cuando estén resguardados o cuando se estén reteniendo para algún propósito.

Según la cláusula 4.3.3 de la norma ISO 27001:2005 sobre Control de registros se dictamina que se tenga un registro de todos los incidentes y desempeño de la empresa para poder almacenar, identificar, proteger y recuperarse de los riesgos de dicho incidente.

En la cláusula 5.1 la norma ISO 27001:2005 acerca de las responsabilidades de la dirección se establece que el responsable deberá cerciorarse del establecimiento de objetivos y planes de seguridad de información, establecer roles y asignar responsabilidades para la seguridad de información, asegurarse que el SGSI ha sido comunicado a los empleados para que estén conscientes de la importancia del mismo, de tal manera que también deberá proporcionar los recursos necesarios para la gestión de seguridad, por último debe decidir los criterios de tratamiento de riesgo y asegurar que se efectúen auditorías internas.

Según la cláusula 5.2.1 la norma ISO 27001:2005 de Provisión de recursos, la organización debe comprometerse a verificar que el proceso de implementación y funcionamiento del SGSI soporte y respalde los requerimientos comerciales, asegurándose también que los controles implementados sean revisados y aplicados correctamente y así, si se produjeran anomalías se deberán corregir inmediatamente. Tampoco debemos dejar de lado que los requerimientos legales, regulatorios y deberes de seguridad contractuales sean ignorados o no tratados. Todo esto con la finalidad de tener un SGSI efectivo todo el tiempo.

A través de la cláusula 5.2.2 la norma ISO 27001:2005 de capacitación, conocimiento y capacidad se exige que para la contratación de personal se deba determinar un perfil de contratación, posterior al mismo se debe establecer si existen necesidades de entrenamiento para las contrataciones seleccionadas y capacitarlas. Sin embargo se debe realizar también una evaluación en la efectividad de sus actividades para comprobar los resultados de la capacitación, así como mantener la información referente a educación, entrenamiento recibido, capacidades adquiridas, experiencia profesional y una calificación del rendimiento de los empleados.

La cláusula 6.0 la norma ISO 27001:2005 de Auditorías internas es muy clara con respecto a la necesidad y obligación de la organización en realizar auditorías internas y externas con el objetivo de revisar el cumplimiento y desempeño de los lineamientos del SGSI establecidos en la empresa. Además la cláusula es muy clara con respecto a que los auditores no deben auditar su propio trabajo para evitar conflicto de intereses. Todas estas acciones impulsan a la mejora continua del sistema.

La clausura 7.0 de la norma ISO 27001:2005 sobre la revisión gerencial hace hincapié en la participación activa de la gerencia en actividades de revisión periódica del SGSI para asegurar su competencia, eficacia y efectividad.

La clausura 8.1 de la ISO 27001:2005 determina el mejoramiento continuo a través de determinadas consideraciones que incrementen la satisfacción de los interesados. Los mecanismos a tomar en cuenta son: las políticas, objetivos, resultados de las auditorias de seguridad, acciones preventivas-correctivas, revisiones gerenciales y el producto de los análisis de eventos monitoreados.

Según la clausura 8.2 de la norma correspondiente a acciones correctivas se debe detectar las no-conformidades (incumplimiento de requisitos), investigar su causa, minimizar o eliminar su riesgo y efectuar acciones preventivas para evitar la

recurrencia del incidente. Para llevar a cabo este procedimiento se exige que la documentación cada uno de los aspectos previamente analizados, además de los resultados obtenidos de las medidas correctivas tomadas.

Y finalmente la cláusula 8.3 de acción preventiva que demanda las acciones pertinentes para eliminar incidentes potenciales, así mismo como la cláusula 8.2 también existen exigencias para la documentación, tales como: identificación de no-conformidades potenciales, determinación e implementación de acciones preventivas, recopilación de resultados y revisiones de las acciones tomadas, y como punto final se debe actualizar el plan de gestión de riesgos con el análisis realizado.

Por último queda mencionar la instauración del SGSI a través de la norma 27001 se pueden distinguir cinco etapas en las que se define: el alcance del SGSI, el establecimiento de políticas de seguridad, documentación, gestión de riesgos y selección y aplicación de los controles previstos por la ISO. Cada uno de estos procesos será especificado con sus respectivas tareas implementadas en los siguientes capítulos.

1.3. Gestión de Riesgos

Para poder profundizar en la gestión de riesgos es necesario conocer primero que es un riesgo. Según la NIST (The National Institute of Standards and Technology), un riesgo es definido como “el impacto neto negativo del ejercicio de una vulnerabilidad, teniendo en cuenta tanto la probabilidad como el impacto de la ocurrencia”. También se lo puede definir como la explotación de una vulnerabilidad por parte de una amenaza latente que puede causar daños a la empresa.

Ninguna empresa puede afirmar que se encuentra exenta de riesgos ya que todos los días las organizaciones tienen que encarar riesgos de diversa índole. Es por esto que la ISO 27001 provee determinados parámetros que una empresa debe cumplir con

respecto al contexto de la administración de riesgos estratégicos a través del cumplimiento de políticas de Seguridad de la Información. Con este conocimiento previo podemos puntualizar que la gestión de riesgos dentro de una organización contempla cada uno de los procesos de planeación, liderazgo, control y organización que favorecen a la minimización o eliminación que pueden producir los riesgos, afectando al cumplimiento de las estrategias de negocio de la organización. Para ello la gerencia organizativa debe seleccionar o definir una técnica de cálculo de riesgos que satisfagan sus necesidades, así como los requerimientos legales y regulatorios de la empresa.

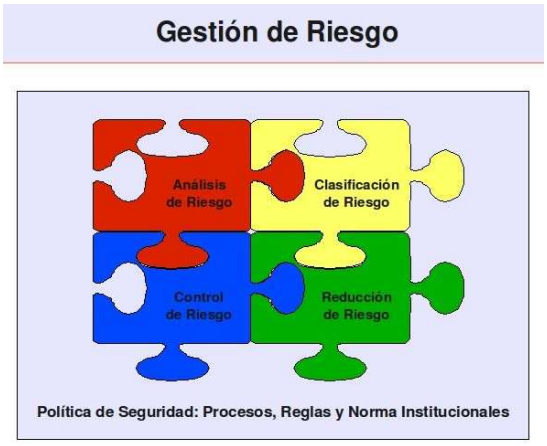


Gráfico 3: Marco de actividades para la gestión de riesgo
http://protejete.wordpress.com/gdr_principal/Gestión_riesgo_si/ enero 18 de 2013

1.3.1. Análisis de Riesgos

Son todas las actividades que comprenden la identificación y valuación de riesgos a través del reconocimiento de amenazas y vulnerabilidades sobre los activos de información. Cada uno de estos riesgos debe estar debidamente relacionado y clasificado de acuerdo a su nivel de impacto y ocurrencia con respecto a los objetivos de la empresa. La medición o valoración de estos riesgos depende del tipo de método que decida utilizar la empresa dependiendo de los requerimientos de la organización. A través de las métricas, se puede priorizar riesgos y establecer métodos de tratamiento que procure que las vulnerabilidades no sean aprovechadas por las amenazas.

1.3.1.1. Clases de Riesgos

Existen diferentes tipos de riesgos que la empresa debe tener a su consideración, puesto que a causa de uno de estos se pueden producir perdidas muy significativas para la empresa, ya sean estas, económicas, humanas u operativas.

Riesgos de Integridad: Aquellos que están asociados con la pérdida de esta propiedad, debido a entradas de datos no validas o alteradas por extraños.

Riesgos de Relación: Hacen referencia al uso correcto de la información para la toma de decisiones, la misma que es Gestiónada por una aplicación informática como por ejemplo las bases de datos.

Riesgos de acceso: Tienen relación con el acceso indebido de intrusos (humanos, software malicioso) que violan la seguridad del sistema aprovechándose de ciertas vulnerabilidades.

Riesgos de utilidad: Son aquellos que se centran principalmente en niveles tales como el sistema de respaldos, planes de contingencia y continuidad de negocio.

Riesgos de infraestructura: La tolerancia de los recursos (humanos, físicos, aplicativos) no es acorde a los requerimientos para el desarrollo y buen funcionamiento de la empresa.

Riesgos de seguridad general: Son todos aquellos estipulados en la norma IEC 950 (International Electrotechnical Commission) sobre instalaciones eléctricas, mecánicas, incendios y radiaciones.

1.3.1.2. Fases del Análisis de Riesgo

El análisis de riesgo consiste en las siguientes fases descritas a continuación:

1.3.1.2.1. Análisis de activos

Es la fase de reconocimiento y valoración de activos, que se consideran valiosos para el cumplimiento de los objetivos de una organización. La preservación de dichos activos asegura el buen funcionamiento y continuidad del negocio, es por eso que la ISO 27001 propone considerar: datos, documentos legales, software, hardware, recursos humanos, imagen y reputación de la compañía, así como los servicios tales como los de redes y comunicaciones, etc.

Tomando en cuenta las consideraciones anteriores, se procede a identificar los requerimientos legales y comerciales a los que los activos están sujetos con el fin de verificar si existen otros activos involucrados además de los ya determinados. El reconocimiento de los requerimientos de seguridad depende de tres fuentes:

- Evaluación de riesgos: amenazas, vulnerabilidades, posibilidad de ocurrencia, impacto al negocio.
- Aspectos legales: requerimientos contractuales.
- Especificaciones de soporte operativo para el procesamiento de información: principios, objetivos, requerimientos

La tasación de activos se realiza a través de una escala de Likert

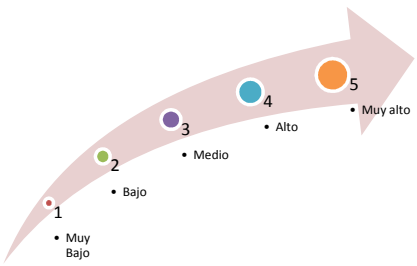


Gráfico 4: Escala de Likert (Nivicela)

Aplicación de la escala de Likert a la tasación de activos de información

Activos de Información	Confidencialidad	Integridad	Disponibilidad	Total
Base de datos clientes	**2**	**5**	**5**	**4**
Internet	**2**	**1**	**3**	**2**
Router's	**1**	**1**	**5**	**2**

Tabla 3: Tasación de activos de información (A. G. Gomez)

Pero la norma también es insistente en la identificación de los propietarios de cada activo, el objetivo de ésta es el de asignar responsabilidades tales como: clasificar activos, otorgar derechos de acceso, establecer sistemas de control y revisión periódica de todas las obligaciones anteriores. La tabla de responsabilidad estará determinada por los activos que se consideren de alta criticidad (nivel alto de pérdida de confidencialidad, disponibilidad e integridad). Además de esto la norma hace mención también a deberes adicionales reglamentarios para documentar e implementar reglas para el uso adecuado de los activos, las mismas que deben ser conocidas y ejecutadas por los empleados como parte su empleo.

Activos de información	Propietarios
Base de datos clientes	Sistemas

Tabla 4: Activos críticos y propietarios (Alan Calder)

1.3.1.2.2. Amenazas

Todos los activos están sujetos a un diferente número de amenazas que pueden generar daños a la organización. Una amenaza puede ser definida como un evento natural, accidental o intencional que puede afectar económica, material u operacionalmente a una organización.

Clasificación de las amenazas:

La Metodología MAGERIT propone un conjunto de amenazas más comunes, que se han presentado para otras organizaciones en diferentes partes del mundo, en este caso únicamente se consideraran las que califican como las que tienen mayor probabilidad de ocurrencia, de acuerdo a la experiencia que se posee del medio en el que se desenvuelve el ambiente de la organización.

Amenazas Naturales [N]

- ✓ [N.1] Fuego: Incendio que puede acabar con los recursos del sistema
- ✓ [N.2] Daños por agua: Inundación que puede provocar daños al sistema
- ✓ [N.3] Desastres Naturales: Incidentes catastróficos que pueden acabar con las instalaciones o parte de ellas, incluyendo los recursos

Amenazas a Instalaciones [I]

- ✓ [I.1] Fuego: Incendio provocado o accidental producto de actividad humana o industrial
- ✓ [I.2] Daños por agua: Filtrados, fugas o inundaciones que pueden provocar daños a los recursos
- ✓ [I.3] Contaminación mecánica: partículas de suciedad, polvo o vibraciones que interrumpen el funcionamiento apropiado de los equipos
- ✓ [I.4] Contaminación electromagnética: Interrupción de señales debido a campos magnéticos, luz UV o interferencias de radio
- ✓ [I.5] Avería de origen físico o lógico: Fallos propios de los equipos o del software instalado
- ✓ [I.6] Corte de suministro eléctrico: Cortes de energía
- ✓ [I.7] Condiciones inadecuadas de temperatura y/o humedad: tolerancia de los sistemas a condiciones de temperatura excesivos.
- ✓ [I.8] Falla de servicios de comunicaciones: falla en la transmisión de datos e información a través de la red, sitios web, correo, etc.

- ✓ [I.9] Interrupción de otros servicios y suministros esenciales
- ✓ [I.10] Degradación de los soportes de almacenamiento de la información
- ✓ [I.11] Emanaciones electromagnéticas

Errores y fallos no intencionados

- ✓ [E.1] Errores de los usuarios
- ✓ [E.2] Errores del administrador
- ✓ [E.3] Errores de monitorización
- ✓ [E.4] Errores de configuración
- ✓ [E.7] Deficiencias de la organización
- ✓ [E.8] Difusión de software dañino
- ✓ [E.9] Errores de re-encaminamiento
- ✓ [E.10] Errores de secuencia
- ✓ [E.11] Escapes de información
- ✓ [E.15] Alteración de la información
- ✓ [E.16] Introducción de información correcta
- ✓ [E.17] Degradación de la Información
- ✓ [E.18] Destrucción de la información
- ✓ [E.19] Divulgación de información
- ✓ [E.20] Vulnerabilidades de los programas (Software)
- ✓ [E.21] Errores de mantenimiento/actualización de programas
- ✓ [E.23] Errores de mantenimiento/actualización de equipos
- ✓ [E.24] Caída del sistema por agotamiento de recursos
- ✓ [E.26] Indisponibilidad del personal

Ataques intencionados [A]

- ✓ [A.4] Manipulación de la configuración
- ✓ [A.5] Suplantación de identidad del usuario
- ✓ [A.6] Abuso de privilegios de acceso
- ✓ [A.7] Uso no previsto
- ✓ [A.8] Difusión de software dañino
- ✓ [A.9] Re encaminamiento de mensajes
- ✓ [A.10] Alteración de secuencias
- ✓ [A.11] Acceso no autorizado
- ✓ [A.12] Análisis de trafico
- ✓ [A.13] Repudio
- ✓ [A.14] Interceptación de información
- ✓ [A.15] Modificación de la información
- ✓ [A.16] Introducción de falsa información
- ✓ [A.17] Corrupción de la información
- ✓ [A.18] Destrucción de la información
- ✓ [A.19] Divulgación de la información
- ✓ [A.22] Manipulación de programas
- ✓ [A.24] Denegación de servicio
- ✓ [A.25] Robo
- ✓ [A.26] Ataque destructivo
- ✓ [A.27] Ocupación enemiga
- ✓ [A.28] Indisponibilidad del personal

- ✓ [A.29] Extorsión
- ✓ [A.30] Ingeniería Social (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

Cada una de estas amenazas intencionales o deliberadas explota las vulnerabilidades del sistema o de las aplicaciones si estas no han sido mitigadas. Reconocidas las amenazas, se procede a evaluar la posibilidad de ocurrencia a través de la escala de Likert (Grafico 4). Las decisiones para descartar o asumir las amenazas deberán regirse de acuerdo a la calificación obtenida según la escala de Likert, considerando que muchas de ellas pueden causar serias consecuencias económicas a la organización.

La posibilidad de la presencia de amenazas es un factor que se puede establecer a través de consideraciones específicas tales como:

Amenazas deliberadas: La posibilidad de que atacantes expertos o que tengan conocimiento se vean atraídos por los valiosos activos.

Amenazas accidentales: Posibilidad de que se produzcan amenazas naturales, se realiza el análisis a través de estadísticas o de la experiencia.

Incidentes del pasado: Posibilidad de reincidencia de alguna amenaza que ya haya sucedido en pasado.

Nuevos desarrollos y tendencias: Los nuevos productos que se publican en internet que pueden ser utilizados para explotar vulnerabilidades.

1.3.1.2.3. Vulnerabilidades

Son debilidades de seguridad del sistema de información que puede permitir a las amenazas causarle daños y generar pérdidas de índole económico, reputacional u operativo a la organización. Estas debilidades se consideran inofensivas por si solas, pero cuando se combinan con las amenazas, pueden afectar negativamente la condición de los activos.

Las vulnerabilidades se pueden clasificar como:

Seguridad de los recursos humanos

- Falta de capacitación sobre seguridad
- Falta de motivación al personal
- Falta de mecanismos de monitoreo
- Falta de políticas de uso correcto de telecomunicaciones
- Falta de políticas de contratación
- Empleados desmotivados
- Carencia de control en la entrega de activos al caducar el contrato
- Llaves de agua abiertas
- Carencia de reglamento interno
- Falta de capacitación de uso del sistema
- Falta de políticas de confidencialidad de información
- Falta de inversión en horas de trabajo del personal
- Falta de mecanismos de monitoreo del personal
- Sobrecarga de trabajo al personal

Control de acceso

- Segmentación de redes incorrecta
- Falta de políticas de uso de aplicaciones y de información
- Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación.
- Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación.
- Mala administración de llaves criptográficas
- Falta de control de acceso físico a oficinas o salones restringidos

Seguridad física y ambiental

- Falta de control de acceso físico a oficinas o salones restringidos
- Ubicación del establecimiento en espacios riesgosos

- Falta de recursos de protección de los equipos de TI
- Carencia de planes de restitución de equipos
- Falta de control del uso y buen funcionamiento de los equipos
- Falta de un sistema contra incendios
- Gotera
- Fuga de agua por daños de cañería
- Instalaciones eléctricas no protegidas
- Almacenamiento de productos inflamables sin adecuaciones
- Falta de condiciones ambientales apropiadas para la protección de los equipos
- Cableado de red inadecuado

Gestión de operaciones y de comunicación

- Uso complicado de interfaces
- Gestión de red inadecuada
- Falta de control de software ilegal
- Falta de conservación de los soportes de información
- Carencia de mecanismos que controlen el envío y recepción de mensajes
- Carencia de políticas de seguridad sobre el copiado de documentos
- Falta de protección en redes públicas de conexión
- No disponer de un ISP adicional
- Falta de validación de datos procesados
- Dispositivos de comunicaciones quemado
- Dispositivos de comunicación mal configurados
- Falta de plan de restitución de equipos

Mantenimiento, desarrollo y adquisición de sistemas de información

- Mala administración de llaves criptográficas
- Políticas incompletas sobre el uso de criptografía
- Falta de validación de datos procesados
- Documentación de software incompleta o mal elaborada
- Carencia de pruebas de software
- Uso complicado de interfaces
- Falta de planes de mantenimiento y limpieza de equipos

- Falta de robustez del sistema
- Falta de manuales de configuración
- Mala administración de la base de datos
- Mala estructuración de la base de datos (A. G. Gomez)

Otros

- Falta de mecanismos de monitoreo
- Carencia de protecciones físicas externas a las edificaciones
- Defectos de fábrica de los equipos
- Apagones por fallos del proveedor de energía eléctrica
- Falta de equipamiento auxiliar en stock
- Falta de plantillas de registro
- Falta de un plan de contingencia en caso de protestas civiles
- Falta de plan de gestión y control de recursos vs requerimientos

1.3.1.3. Impacto de riesgos

Luego de considerar la clasificación de vulnerabilidades, se debe determinar la posibilidad de que estas debilidades sean explotadas por las amenazas. Para que se produzca un incidente que pueda dañar los activos, las amenazas y vulnerabilidades deben presentarse juntas. Es por eso que la norma ISO 27001 propone que se realice sobre ellas un cálculo de la posibilidad de ocurrencia y el posible impacto, abarcados dentro del cálculo del riesgo, proceso que sostiene el análisis y la evaluación del mismo. Este cálculo es llamado también el valor económico del riesgo sobre un activo.

El proceso de análisis de riesgos consiste en el reconocimiento y cálculo de riesgos sujetos a los activos identificados y al cálculo de las amenazas y vulnerabilidades. No existe un método exigido por la norma, sino que se da apertura a que sea la organización la que decida como calcular el riesgo, de manera que cumpla con los requerimientos de seguridad de la empresa. El propósito de calcular el riesgo es que a través de los niveles obtenidos se puede priorizar los riesgos que son más problemáticos para la organización.

Es recomendable que el factor de impacto de riesgo sea determinado a través de la tasación de riesgos, que es un método que trata de relacionar el coste de la amenaza y la posibilidad de ocurrencia de la misma (Gráfico 4: Escala Likert).

Se deben considerar los siguientes factores:

Activo	**Amenaza**	**Impacto de la amenaza**	**Frecuencia de ocurrencia**	**Medición de riesgo**	**Priorización**
Base de datos cliente	Acceso no autorizado	5	3	15	3
Base de datos cliente	Modificación de la información	5	2	10	2
Base de datos cliente	Introducción de falsa información	4	2	8	1

Tabla 5: Método de cálculo de riesgo (A. G. Gomez)

La medición del riesgo es un factor calculado dado por:

$$Medición\ del\ riesgo = Impacto\ de\ la\ amenaza * Frecuencia\ de\ ocurrencia$$

(A. G. Gomez)

El proceso de evaluación de riesgo consiste en conocer cuál es la amenaza que provoque un riesgo más significativo para la organización. La norma reconoce que para fijar los niveles de riesgo se debe considerar el impacto económico, tiempo de recuperación, posibilidad de ocurrencia y la posibilidad de obstruir la continuidad del negocio. Desde aquí la Gerencia puede tomar las decisiones respectivas, sabiendo cuales son los riesgos que pueden ser asumidos, los que deben ser transferidos y los que pueden ser tratados mediante un plan (Controles del estándar). Sin embargo no se debe pasar por alto la exigencia de la norma ISO 27001 a través de la cláusula 4.3.1, a través de la cual los procesos de análisis y evaluación de riesgo deben estar correctamente documentados como informe de medición del riesgo.

1.3.1.4. Riesgo Residual

A pesar de todas las medidas que se tomen para tratar los riesgos, siempre queda una porción de riesgo que no se ha cubierto con el plan. Estos remanentes son considerados difíciles de calcular pero deben ser evaluados y tomados con precaución para asegurarse de que sean suficientemente protegidos. Este nuevo nivel de riesgos es calculado como los riesgos anteriores, pero esta vez considerando que muchos de los recursos ya están protegidos. El cálculo de riesgo residual es un proceso cíclico, en cuanto se logra cubrir el riesgo se deberá volver a realizar el análisis para poder tener asegurada la minimización o eliminación del riesgo.

Se debe tener en cuenta que para cubrir algunos riesgos se necesita una alta inversión económica, por lo que se debiera meditar en asumir el riesgo puesto que en algunos casos es menos costoso el daño que el control del mismo. Por otro lado existen otras opciones tales como la transferencia de riesgos a otras entidades dedicadas a ello (aseguradoras), esto para los riesgos que no pueden ser evitados. Lo que siempre se debe tener en mente es que se debe priorizar los riesgos sobre los activos que resulten esenciales para el normal funcionamiento de la organización.

Debido a que la empresa sufre cambios estructurales y organizativos durante su trayecto, se debe procurar realizar una evaluación periódica de todos los riesgos, incluidos los residuales. Se debe tener claro que todos estos procesos documentados también forman parte de las exigencias de la norma ISO 27001.

1.3.2. Tratamiento de Riesgo

Una vez realizados los análisis y evaluaciones pertinentes se entra en un proceso de toma de decisiones sobre los riesgos latentes de los activos. Para cumplir con este proceso de detección y prevención de riesgos es conveniente la implementación de controles (propios o de la norma), aunque, sin embargo se debe tomar en cuenta que adicionalmente existe la aceptación y transferencia del riesgos.

La alta gerencia deberá considerar prioritariamente el valor resultante de dos factores fundamentales determinados previamente como son: el impacto si el riesgo llega a producirse y la posibilidad de ocurrencia del mismo. A través de estos factores se puede prever la pérdida estimada de la organización en caso de no reprimir el riesgo. No obstante de entre todos los riesgos existen los de seguridad de la información, que son un poco impresos en cuanto a la frecuencia de ocurrencia, por lo que es recomendable tratarlos con suma cautela al momento de aceptar o mitigar el riesgo.

1.3.2.1. Estrategias de tratamiento de riesgos

Las estrategias de tratamiento de riesgo se pueden considerar como un tipo de defensa, salvaguarda o medida de seguridad que a través de cualquier medio intenta minimizar o mitigar el impacto del riesgo sobre una organización. Existen dos medidas que se pueden utilizar:

- **Medidas de seguridad activas de prevención y detección**: a través de evitar el riesgo, reducir del riesgo.
- **Medidas de seguridad pasivas o de corrección**: Aceptación y transferencia del riesgo.

Gráfico 5: Tratamiento de Riesgos

Los controles más comunes utilizados para la seguridad de información al margen de las estrategias de tratamiento de riesgo son:

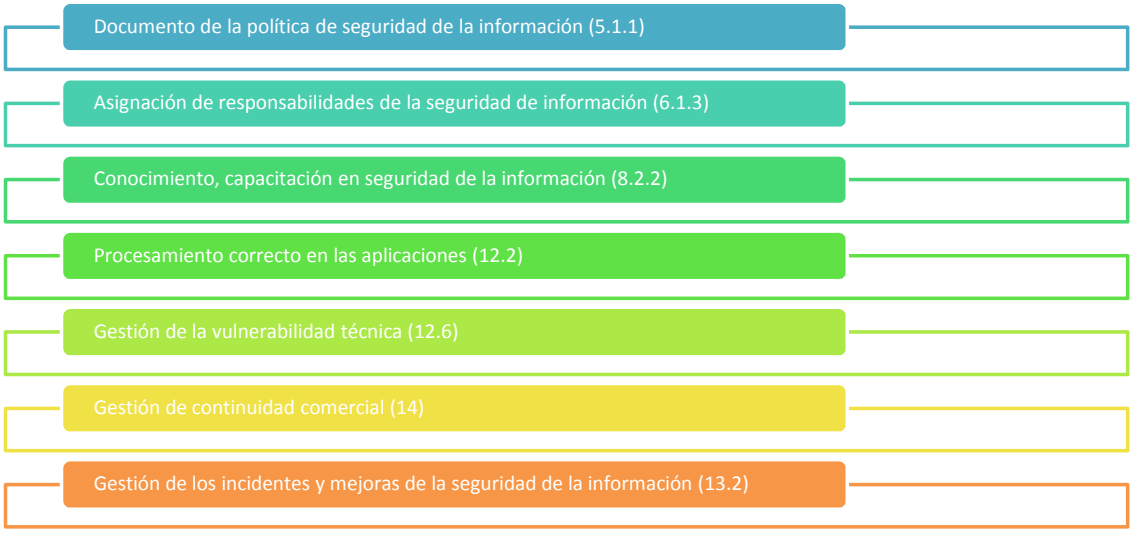


Tabla 6: Controles comunes de un SGSI (A. G. Gomez)

La utilización de cada uno de estos controles deberá tener una justificación de su uso, al igual que los controles que no sean considerados. Este procedimiento tiene el objetivo de mostrar a la empresa que todos los controles han sido estimados.

Por otro lado las decisiones de la organización con respecto a las medidas, deberán estar sujetas al coste económico que implique la medida, la dificultad de implementación técnica, humana y organizativa, así como de la efectividad de la medida adoptada sobre el riesgo potencial.

Reducción de riesgo*:* Consiste en reducir el riesgo a niveles aceptables. Existen dos formas de reducir el riesgo, la primera es mediante la reducción de la posibilidad de que la vulnerabilidad sea explotada y la segunda es mediante un plan de contingencia, donde el impacto del riesgo es reducido. Se puede aplicar cualquier modo o la combinación de ellos, todo dependerá de los requerimientos de negocio, ambiente, y la necesidad de operativa de la empresa.

Como se ha anticipado previamente, no existe un criterio de selección universal de controles aplicables, sino más bien la decisión dependerá del resultado de las discusiones entre integrantes clave de la organización, los mismos que deberán tomar en cuenta la importancia de los activos, inversión, cultura y la tolerancia al riesgo de la empresa.

La norma ISO 27001 ofrece una serie de controles o lineamientos que pueden ser implementados y se los puede encontrar más adelante en el Capítulo 6: Políticas de seguridad.

Aceptación de riesgo*:* Es utilizado cuando el riesgo es intratable debido a que no se puede encontrar controles que puedan mitigar el riesgo, o que la aplicación del control tenga un costo mayor al que puede producir el riesgo, por lo que la organización asume las consecuencias del acontecimiento. La decisión de aplicabilidad debe estar correctamente documentada y aprobada por la gerencia según lo exigen las clausulas 4.2.1 y 5.1 del ISO 27001:2005, especificando claramente los criterios de aceptación del riesgo.

Transferencia de riesgo*:* Cuando se nota que la reducción o mitigación del riesgo es complicada se recurre a la transferencia del riesgo a terceras empresas, que generalmente se dedican a este tipo de actividades (aseguradoras) y resultan más económicas, sin embargo los contratos con las aseguradoras se deben tratar con mucho cuidado, puesto que existen términos y condiciones que estas empresas imponen según la situaciones que se presenten. De modo usual se conoce que las aseguradoras no mitigan los impactos no financieros o inmediatos de un evento problema, dejando así riesgos residuales, por lo que también se puede optar por transferir el riesgo de manejo de activos o procesos críticos a terceros capaces de manipular de modo seguro este tipo de elementos.

El problema de este método radica en que la seguridad de información y de las instalaciones depende de la empresa que contrata los servicios, por ende también la estimación y gestión de nuevos riesgos.

Evitar el riesgo*:* Se opta por esta decisión cuando es posible contrarrestar el riesgo a través de cambios metódicos en el desarrollo y desempeño de actividades. Se disponen de medios para evitar los riesgos tales como: No desarrollar ciertas actividades (uso del internet), mantener los activos en áreas seguras, no procesar información sensible. Habitualmente todo esto regido a los requerimientos, tanto como necesidades financieras y comerciales.

1.3.2.2. Plan de tratamiento de riesgos

Es un proyecto, donde se lleva a cabo la ejecución de tareas que ayudan a cumplir con las decisiones tomadas por la organización. Estas tareas tienen que haber sido definidas, planificadas, de manera que se pueda entonces asignar responsables, recursos a utilizar, los entregables, fechas críticas y monitoreo de cumplimiento de actividades. Conviene sin embargo advertir que como se trata de un proyecto, implica mucha responsabilidad, por lo que se aconseja asignar este proyecto a una persona responsable, idónea, que sepa controlar el desempeño del proyecto y el manejo preciso de los recursos a utilizar. El jefe de proyecto deberá encargarse de cumplir principalmente con actividades fundamentales como:

- Establecer limitantes del proyecto y estrategias para debilitarlos.
- Priorizar tareas del proyecto.
- Identificar fechas de entrega e hitos del proyecto.
- Estimar los recursos y sus requerimientos.
- Identificar ruta crítica del proyecto.

Una de las herramientas más usadas y recomendadas para la planificación de estas actividades es el diagrama de GANTT. Una vez organizado el diagrama se deben asignar los recursos y acciones que harán que las decisiones para el tratamiento de riesgos se sinteticen. Todas estas concepciones se encuentran definidas en la cláusula 4.2.2 de la ISO 27001.

No debemos olvidar la importancia de llevar a cabo periódicamente el mantenimiento, monitoreo, revisión y revaluación de riesgos, como del SGSI, puesto que la empresa siempre se encuentra en un estado cambiante y evolutivo, produciendo cambios en los activos, incrementando el número de amenazas y vulnerabilidades, etc., por lo que el Gobierno de TI se verá en la obligación de permanecer constantemente realizando cambios y adecuaciones al plan de gestión de riesgos, como a todos sus niveles previos de análisis, evaluación, definición de objetivos y controles establecidos. Vale la pena resaltar que aunque la empresa no experimente cambios de infraestructura se debe validar que los controles actuales se estén cumpliendo y estén rindiendo un desempeño satisfactorio.

1.3.3. Herramientas para el análisis de riesgos

Con el propósito de facilitar la gestión de riesgos se han creado varias herramientas o metodologías que apoyan a su causa. Entre ellas podemos encontrar herramientas comerciales y no comerciales, cada una con un mismo principio, pero con enfoques diferentes. La decisión dependerá de las necesidades y requerimientos de la organización.

1.3.3.1. Herramientas comerciales y gratuitas

Herramientas Comerciales

CRAMM (CCTA Risk Analysis and Management Method): Es una metodología software que proporciona los parámetros técnicos y no técnicos para la evaluación de riesgos de los sistemas de información. Fue creada por la CCTA (Central Computer

and Telecomunication Agency) de Reino Unido y es una herramienta totalmente compatible con la norma ISO 27001.

Su proceso de trabajo consiste en tres etapas:

- Identificación y valoración de activos: activos físicos y lógicos
- Análisis de amenazas y vulnerabilidades: hacking., virus, fallas técnicas o lógicas, daños intencionales, errores comunes, entre otros.
- Selección y recomendación para el tratamiento de riesgo: Utiliza un banco de 3000 medidas propias.

Gráfico 6: Funcionamiento CRAMM (Tangient LLC)

COBRA (Consultative, Objetive and Bi-functional Risk Analysis): Es una aplicación software que provee lineamientos de la norma ISO 17799 para la auditabilidad de un Sistema de gestión de seguridad de la información. Su servicio es compatible con otras metodologías reconocidas. Ofrece:

- Flexibilidad modular al separar su proceso por etapas, lo que garantiza mayor precisión en los resultados y soluciones.
- Personalización automática a través de la alimentación de una base de conocimientos que puede ser incorporado por el encargado de la gestión de riesgos.
- Considerado auto analítico debido a su facilidad de uso, no se necesita ser experto para poder manejar este software.

- Las soluciones propuestas son calculadas automáticamente por tanto proporciona soluciones rápidamente y que pueden considerarse efectivas.
- Genera reportes profesionales que pueden ser claramente interpretados por la alta gerencia.

RISKMASTER: Es un software que plantea el uso de lineamientos de la norma ISO 17799 para la evaluación de riesgos. Está basado en buenas prácticas tales como la ISO 27001, NIST 800-53 y COBIT IV. Utiliza plantillas predefinidas y posee una interfaz intuitiva, por lo que no es necesario un experto para manejar este sistema. Se lo puede encontrar en versiones web, de escritorio y para servidores.

Herramientas y Metodologías gratuitas

MAGERIT: Es una metodología para el Análisis y Gestión de Riesgo de Sistemas de Información cuyo propósito es de concientizar a los propietarios de los sistemas de Información, ofrecer un método eficaz para la gestión de riesgos, ayudar con la generación de un plan de acción para controlar riesgos y facilitar procesos tales como: certificación, auditoria, acreditación y evaluación interna.

OCTAVE (Operationally Critical Threat, Analysis and Vulnerability Evaluations): Es una herramienta de software libre que facilita la evaluación de riesgos, se centra específicamente en la planificación y consultoría estratégica de riesgos de seguridad.

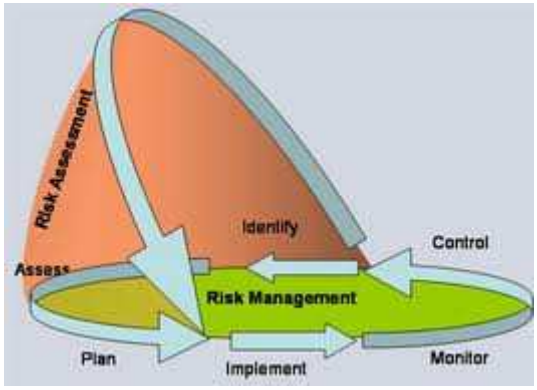


Gráfico 7: Procesos que engloba OCTAVE (Security Managment Consulting International)

Estas y otras herramientas pueden ser utilizadas para la Gestión de Riesgos, pero en este caso se ha seleccionado la metodología MAGERIT, cuyos métodos serán de ayuda para el desarrollo del Plan de Gestión de Riesgos para MADECO Cía. Ltda.

1.3.3.2. MAGERIT

Esta herramienta fue elaborada por la CSAE (Consejo Superior de Administración Electrónica), su creación se debió al nivel elevado de tecnologías de información al que están sujetas las Administraciones para el cumplimiento de sus objetivos. Por lo que se puede decir que esta metodología está orientada a proporcionar métodos que ayuden a Gestiónar recursos electrónicos, informáticos y telemáticos con el objetivo de controlar los riesgos de seguridad de información.

A través de MAGERIT los encargados de información automatizada tienen la capacidad de valorar la información y servicios que prestan. La valoración sirve para decidir acerca de cómo proteger aquellos recursos considerados fundamentales.

Es necesario conocer los riesgos a los que están sometidos los activos de información de una organización, puesto que a través de ello podemos establecer un plan de acción que minimice el impacto que puede producir una amenaza o el riesgo latente. Es por ello que se han aparecido varias guías que soporten este proceso, lamentablemente todas ellas basadas en aproximaciones de las cuales existe una preocupación, puesto que si no se consideran todos los elementos de forma estricta, los resultados serían poco fiables. Debido a esto, esta metodología busca una aproximación más exacta que no posea conclusiones improvisadas, ni opiniones inocuas del analista.

Actualmente se puede constatar que todas las organizaciones cuentan con un conjunto de sistemas de información en el que se deposita toda la confianza para el cumplimiento de sus objetivos empresariales, no obstante el tema de la seguridad en este caso es fundamental. La interrogante de los afectados es, si su sistema es confiable o si la inversión que realizan realmente se ve proyectada a través de un

control de fallos. En consecuencia lo que busca MAGERIT es conocer los riesgos sobre los activos de mayor valoración, para poder así encararlos y controlarlos.

1.3.3.2.1. Objetivos de MAGERIT

Los objetivos directos de la herramienta son concienciar a los responsables de los sistemas de información sobre la importancia de considerar riesgos y cómo actuar a tiempo en contra de ellos, ofrecer procedimientos metódicos para el análisis de riesgos, brindar parámetros para descubrir y planificar acciones que ayuden a controlar los riesgos. En cuanto a los objetivos indirectos, se refieren a la preparación de la organización para procesos de auditoria, certificación, control interno o acreditación. Finalmente pero no menos importante MAGERIT también busca una cierta estandarización en cuanto a documentación de gestión de riesgos, los mismos que se reconocen como:

- Modelo de Valor: Valoración y dependencia entre activos de la organización.
- Mapa de riesgos: Activos sujetos a amenazas.
- Evaluación de salvaguardas: Apreciación de la eficacia de los controles aplicados a los riesgos.
- Estado de riesgos: Estimación de los efectos del riesgo residual.
- Informe de insuficiencias: Carencia o debilidad de los controles de riesgo.
- Plan de seguridad: Programación específica de actividades que servirán para la gestión de riesgo.

1.3.3.3. Administración MAGERIT

La metodología propone determinadas técnicas y consideraciones para crear, desarrollar y mantener un Plan de Gestión de Riesgos. Se ha dividido el proceso en tres etapas:

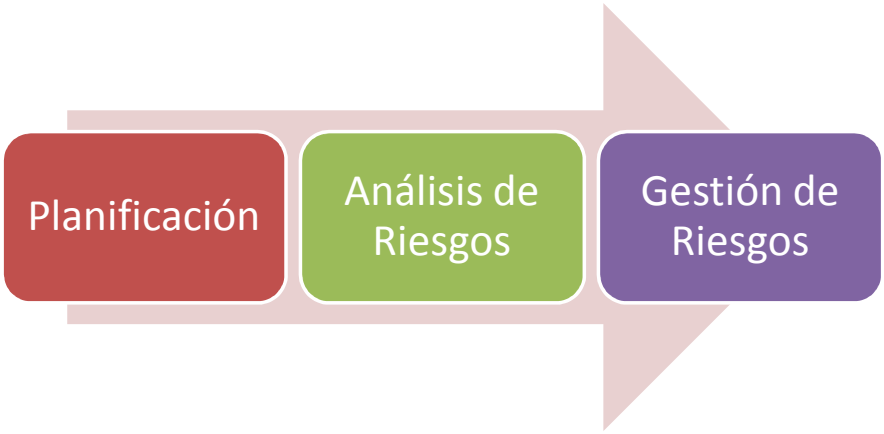


Gráfico 8: Proceso del Análisis y Gestión de Riesgos

(Nivicela)

Cada una de las etapas conlleva en si un conjunto de actividades, las cuales se estructuran en forma de tareas. Se estima que cada tarea implica cierta dificultad, sin embargo la metodología se encarga de indicar como llevar a cabo con éxito cada una de ellas. Es por ello que se establecen tres conceptos para la resolución de cada tarea: acciones a realizar, técnicas recomendadas para llevar a cabo a buen término los objetivos de cada tarea, participantes, afectados del cumplimiento de cada acción, datos de entrada y salida (productos y documentos a obtener). Y es así que para tener un seguimiento adecuado del proyecto se llevará un listado de cumplimiento de hitos, hasta finalizar el proyecto.

Asignación de responsabilidades

Se recomienda que la organización posea una estructura organizativa ordenada que cumpla con determinadas funciones durante todo el proceso de instauración y desarrollo del proyecto. Posterior a la asignación de las diferentes responsabilidades se procede a definir el modo en el que se va a desarrollar el proyecto. El desarrollo del AGR (Análisis y Gestión de Riesgos) consiste en estructurar el proyecto para que sirva de guía para los usuarios y responsables del equipo de trabajo. Además se establece un conjunto de productos, técnicas, funciones y responsabilidades que definen el marco de trabajo.

Se sugiere la siguiente estructura:

Roles	**Perfil**	**Responsabilidad**
Comité de Dirección	Directivo de alto nivel Conocimiento de las estrategias y objetivos de negocio.	Asignar recursos necesarios para el proyecto
		Aprobar resultados finales de cada proceso
Comité de Seguimiento	Responsables de las unidades afectadas Responsables de la informática y gestión RRHH Administración, etc.	Resolver incidencia durante el desarrollo del proyecto
		Control de personal con el perfil adecuado para el desarrollo del proyecto
		Aprobar informes intermedios y finales de cada proceso
		Elaborar informes finales para el comité de dirección
Equipo de proyecto	Personal con conocimiento en seguridad de la información, tecnologías y gestión de riesgos	Llevar a cabo las tareas del proyecto
		Recopilar, procesar y consolidar datos
		Elaborar informes
Grupos de interlocutores	Usuarios de las unidades afectadas: responsables de servicios internos, personal de explotación y operación de servicios	

	informáticos	
Promotor	Posee visión global de los SI y su papel en las actividades de la organización.	Lidera las primeras tareas del proyecto
Director de proyecto	Directivo de alto nivel	Seguridad dentro de la Organización(SI)
		Planificación de servicios
		Coordinación de servicios
Enlace Operacional	Interlocutor visible del Comité de Seguimiento Conocimiento de las personas y unidades implicadas.	Conectar al equipo de proyecto con el grupo de usuarios.

Tabla 7: Segmentación de la estructura organizativa
(Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

Descripción de los procesos

Los siguientes procesos no son secuenciales, pero particularmente se empieza por la planificación, en cuanto al análisis y gestión de riesgos, estos se retroalimentan según sea necesario.

Los procesos son los siguientes:

Planificación

El lanzamiento del proyecto se da a partir de este proceso, que es el de establecer las consideraciones necesarias para poder iniciar, investigar las oportunidades, definir objetivos y dominio que se va a abarcar, al igual que planificar recursos materiales y

humanos. Siendo su principal objetivo el de establecer un marco general de referencia para el proyecto. Así mismo también busca concienciar al alto mando gerencial para exponer las oportunidades del desarrollo de un SGSI. Y así finalmente para lograr exponer la decisión aprobada de la Dirección y así crear el ambiente necesario para el del proyecto.

De esta etapa se distinguen las siguientes actividades

1. **Estudio de oportunidad**

   Se trata de encontrar la oportunidad de realizar el proyecto con fecha actual. Para lo cual se utilizaran técnicas tales como entrevistas y reuniones, de donde se obtendrá el informe preliminar para elaborar el proyecto, sensibilización del personal, apoyo de la dirección y designación del comité de seguimiento, cuyo participante central es el promotor.

   El informe preliminar deberá contener la recomendación para el desarrollo del proyecto de Gestión de Riesgos junto con su justificación, un informe de la situación actual de la empresa en cuanto a seguridad, aproximaciones de los medios y dominios a incluirse. Este documento será desarrollado y entregado a la Dirección por el promotor para su aprobación, modificación o retraso del proyecto.

2. **Determinación del alcance del proyecto**

   Posterior a la aceptación del proyecto por la Dirección se establecen los objetivos, restricciones, se determina el dominio y límites del proyecto, así también se identifica el entorno, se estima las dimensiones y el coste-beneficio que va a implicar su desarrollo. En esta etapa se especifica la extensión de las actividades y el plazo de duración el SGSI. Se conoce que el resultado de este proceso serán los objetivos específicos y las limitaciones generales en cuanto a las unidades incluidas dentro del dominio considerado junto con sus roles, es por ello que previamente se debe analizar toda la documentación de la

organización(diagramas de procesos). El comité de seguimiento juega un papel importante durante este proceso, al igual que el director de proyecto designado.

El alcance del SGSI puede ir desde la protección de un proceso a la protección global de la empresa, esta concepción será una disposición de la Dirección.

Por otro lado se pueden distinguir ciertas restricciones a considerar tales como:

a. Políticas o gerenciales
b. Estratégicas
c. Geográficas
d. Temporales
e. Estructurales
f. Funcionales
g. Legales
h. Relacionadas con el personal
i. Metodológicas
j. Culturales
k. Presupuestarias (Públicas)

3. Planificación del proyecto

Se establecen los parámetros de recopilación de información, es decir quiénes serán los entrevistados, cuáles son sus actividades y a que grupo de trabajo han sido asignados. Por lo que los resultados de esta actividad serán: plan de trabajo y procedimientos de gestión de los activos reconocidos con la especificación de los

materiales necesarios para su desarrollo. Además cada una de las actividades deberá constar en un cronograma con su respectivo plazo de elaboración.

El director de proyecto será el encargado de planificar el proyecto de manera que a través de lo establecido en el alcance del proyecto les ayude a determinar el plan de entrevistas, informe de cargas y la vinculación interna de los participantes en los grupos interlocutores, para que de esta manera el comité de seguimiento pueda Gestiónar y aprobar cada proceso desde el punto de vista técnico. Adicionalmente se debe contar con la participación del equipo del proyecto para que coopere con el desarrollo del proyecto.

4. Lanzamiento del proyecto

Se preparan todos los recursos físicos (materiales), lógicos (planes y técnicas para la evaluación y gestión de riesgos) y humanos, por lo que se pone en conocimiento a los afectados sobre la finalidad del proyecto y su participación en el mismo. Se pretende acoplar el conjunto de cuestionarios en la recogida de información (activos y amenazas) con su respectiva valoración, de manera que a través de MAGERIT se pueda trabajar los problemas de seguridad existentes. Tanto el director de proyecto, el comité de seguimiento, el enlace operacional y equipo de proyecto son parte fundamental durante el desarrollo de este proceso.

Se conoce también que de esta etapa saldrán ciertos documentos que acreditaran que se ha pasado por este proceso: Tipología de activos, Dimensiones de seguridad relevantes, criterios de evaluación.

Análisis de Riesgos

Se requiere de un levantamiento de activos, relación de dependencia y valoración, identificación de amenazas, salvaguardas, impactos y pérdidas económicas sobre los activos. Finalmente la interpretación de toda esta información para poder transformarla en un plan de Gestión de Riesgos a ejecutar.

En esta etapa se deberán realizar las siguientes actividades:

1. **Caracterización de los activos**

   El propósito de esta actividad es determinar y valorar activos por la importancia que implican para la organización, para lo cual se deberán realizar tareas tales como identificación de activos, reconocimiento de la dependencia entre activos, y valoración de activos.

   Todos los inventarios (datos manejados, equipamiento físico y lógico), procesos de negocio, diagramas (uso, flujo de datos), caracterización funcional de los puestos de trabajo, locales y sedes de la organización deben formar parte de la información de entrada para su procesamiento, cuyo producto final a obtener es un modelo de valor.

   Todo lo mencionado anteriormente se lo puede lograr a través de diagramas, entrevistas y reuniones en las cuales deberán participar el equipo de proyecto y el grupo de interlocutores. Además se deberá contar con la colaboración del comité de seguimiento y la Dirección para tratar el asunto referente a la valoración de activos.

2. **Caracterización de las amenazas**

   Al igual que se realizó con los activos, el objetivo de esta actividad es identificar y valorar las amenazas, pero adicionalmente en este caso se las valora según la pérdida económica y estratégica que suponga su ocurrencia.

   Se trata de lograr conseguir la relación de amenazas posibles que a través de catálogos de amenazas, arboles de ataque y aplicando los métodos de sensibilización y comunicación con los miembros de las unidades afectadas. El

informe que se desea obtener es el mapa de riesgos (amenazas: frecuencia de ocurrencia, degradación que puede causar) proporcionado por el equipo de proyecto y el grupo de interlocutores participantes.

3. Caracterización de las salvaguardas

Se pretende seleccionar un conjunto de salvaguardas que van a actuar para controlar, minimizar o mitigar las amenazas identificadas de manera más eficaz, es por ello que para esta actividad se debe poseer inventarios, planes de formación, contratos, definición de puestos laborales y acuerdos de externalización de servicios con los cuales se quiere obtener una relación entre todas las salvaguardas desplegadas y de la misma forma que en la actividad 3 aplicamos el procedimiento de socialización para así finalmente definir el informe de evaluación de salvaguardas.

4. Estimación del estado del riesgo

Durante este proceso se estudiarán los informes resultados de las actividades previas, con lo cual se realizarán informes de estado de riesgo e insuficiencias, documentos que deberán contener estimaciones de riesgo e impacto (potencial, residual) y el reconocimiento de deficiencias en el sistema de salvaguardas.

De todo lo detallado anteriormente se deberán emitir los siguientes documentos: Modelos de valor, mapa de riesgos, evaluación de salvaguardas, estado de riesgo, informe de insuficiencias.

Gestión de Riesgos

En esta etapa se seleccionan las estrategias y salvaguardas para mitigar los riesgos, se determina la calidad necesaria para las salvaguardas y luego de emitido el plan de seguridad se lo ejecuta. Por lo que posteriormente se deberán realizar las siguientes actividades:

1. Toma de decisiones

Es aquí donde las conclusiones técnicas expuestas en el análisis de riesgos se convierte en decisiones aplicables cuya única tarea es la de calificar los riesgos. Se debe tener plena precaución con los elementos de entrada para el proceso, así los elementos legislativos, de jurisprudencia, reglamentarios, acuerdos, contratos, informes de medio ambiente y estudios de mercado, puesto que de ello depende la toma de decisiones, las cuales deben ser tomadas desde el punto de vista gerencial y mas no del técnico. Para esta actividad se deberá contar con la participación del equipo de proyecto, el comité de seguimiento y el de dirección.

2. Plan de seguridad

Esta actividad comprende en transformar las decisiones aplicables en acciones concretas en tiempos establecidos, por lo que se debe cumplir con la tarea de realizar programas de seguridad y planes de ejecución. Para concretar las decisiones de manera adecuada y para que beneficie a la organización, se debe considerar la revisión del proceso de análisis de riesgos y de coste beneficio. Es así que además que durante esta actividad se deberá contar con la presencia del equipo de proyecto y del especialista en seguridad.

3. Ejecución del plan

Finalmente se debe materializar cada uno de los proyectos definidos en el plan de seguridad con la finalidad de lograr implantar las salvaguardas, definir normas de uso y operación, mantener el modelo de valor y el de riesgos actualizados junto con un sistema de indicadores de eficiencia y eficacia de desempeño de los objetivos de seguridad que se pretenden.

CAPITULO 2: SITUACION ACTUAL DE LA EMPRESA

MADECO es una compañía limitada dedicada a la venta de materiales de construcción, cuenta con cuatro almacenes en la ciudad de Cuenca. La matriz principal se encuentra ubicada en la calle Guapondélig frente al cementerio Municipal, donde se encuentran las oficinas principales con su respectivo centro de procesamiento de información. Actualmente cuenta con 16 empleados que se encuentran desempeñando diferentes labores en pro del desarrollo de la empresa.

2.1. Misión, visión y objetivos de la empresa

Misión

Dado que el Plan de Gestión de Riesgos contempla todos los procesos cruciales de negocio, se ha recopilado la información referente a la misión de la empresa. Dicha información nos permitirá saber cuál será el alcance del Plan de Gestión de Riesgos. La misión de MADECO se define como:

“Proveer materiales de calidad, durables, a un precio y cantidades justas. Asesorar a nuestros clientes en su compra para que mediante ella contribuyan a su bienestar y tranquilidad y a su vez al desarrollo de la infraestructura y economía del Ecuador.”

Al momento del análisis la empresa no contaba con sus metas de negocio definidas, pero conforme se ha dado el avance del proceso de Análisis Inicial para la creación del Plan de Gestión de Riesgos se ha tenido la colaboración de la Gerencia y de la Dirección General en cuanto a la provisión de esta información.

Visión

Acorde a la ISO 27001:2005 se deberá adquirir conocimiento de la Visión de la empresa para proyectar el Sistema de Gestión de la Seguridad de la Información no solo al cumplimiento de los objetivos presentes de empresa sino también ayudar a cumplir sus objetivos proyectados a largo plazo. Es por eso que la información provista por la Gerencia sobre la visión de la empresa ha sido la siguiente:

"Ser líder y referente en proveer acabados para la construcción en la zona sur del Ecuador."

Objetivos

Para determinar cuáles son los procesos críticos de negocio que deben ser protegidos, la norma ISO 27001:2005 a través de MAGERIT dispone de una técnica para su selección, la que dependerá específicamente de los objetivos que la organización persiga (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II), por lo que la Gerencia ha desarrollado los siguientes objetivos:

"Reducir costos de infraestructura sub-utilizada para obtener el mayor beneficio y mejor relación costo-precio en un plazo no mayor a 3 años.

Renovar exhibiciones y mejorar procesos para la venta incluyendo catálogo web en un plazo no mayor a 1 año."

2.2. Infraestructura de la información

Debido a la falta de definición de los procesos de la empresa se ha tenido que realizar un levantamiento de procesos, cuyo reconocimiento se hizo bajo la autorización del Directorio y de la Gerencia. El levantamiento de procesos se llevó a cabo a través de la realización de entrevistas a cada área, en donde se llegaron a determinar los siguientes procesos: Véase Anexo 2

DEPARTAMENTO/PROCESO	SUBPROCESOS
Alta Dirección: Gerencia	Gestión Administrativa
Ventas	Ventas
	Atención al Cliente
Compras	Compras
Bodega	Despacho de mercadería
	Almacenamiento de Mercadería
	Control de Inventarios
Transporte	Entrega de pedidos
Cómputo y Sistemas de información	Planificación y Organización de Proyectos
	Adquirir e implementar
	Desarrollo, entrega y Soporte
Alta Dirección: Presidencia	Auditoría y Control de procesos críticos de negocio
	Coordinación Principal
Finanzas	Proceso Contable
Alta Dirección: Dirección y Control	Dirección y Control
	Gestión de Recursos Humanos

Tabla 8: Resumen Infraestructura de Procesos
(Nivicela)

En base a la información recolectada vamos a analizar los procesos, recursos e información que es de mayor impacto en los factores críticos de éxito de la empresa, es por eso que la norma ISO 27001 recomienda usar una matriz de despliegue con la finalidad de determinar cuáles son los procesos críticos de negocio.

Los procesos críticos de negocio serán analizados en función de un conjunto de factores críticos de negocio, que serán eventualmente proporcionados por la gerencia de la empresa. Los factores críticos de negocio son definidos como un indicador para la medición de rendimiento desde las perspectivas: financiera, del cliente, interna, innovación y aprendizaje. (Arjona Torres)

2.3. Análisis actual del Sistema de Seguridad de la Información

Para determinar el estado actual de la empresa en cuanto a Seguridad de la Información vamos a desglosar toda la estructura organizacional

Estructura Organizacional

Dentro de la infraestructura organizacional se pueden distinguir las siguientes áreas o unidades de la organización:

Directorio: Supervisión, organización, gestión de recursos humanos, capacitivos y colaboración con la Alta Gerencia.

Presidencia: Administración, coordinación, Auditoría y control de procesos de negocio.

Gerencia: Monitoreo, control de procesos de negocio y gestión Capacitiva.

Unidad de Ingeniería en Sistemas: Mantenimiento, administración, supervisión de equipos y desarrollo de software para la empresa.

Unidad de Contabilidad:

1. Validar que la información de libros y registros contables sean exactos.
2. Asegurar el cumplimiento fiscal de las leyes y regulaciones estatales.
3. Elaborar, analizar e interpretar los estados financieros.
4. Proporcionar a la Gerencia información ordenada, clara y oportuna para la toma de decisiones.

Unidad de Compras: Cotizar productos, pedidos, verificación de la calidad de los productos adquiridos, emitir informes de proveedores.

Ventas: Conocer, ofrecer los productos a los clientes y registrar sus procedimientos en el sistema.

Bodega: Manejo del sistema de inventarios y del movimiento de las existencias dentro del almacén.

Transporte: Transportar los pedidos a los clientes y difundir la imagen de la empresa (Entrega de panfletos).

De la presente descripción y de los procesos que cumplen cada área o unidad se ha podido estructurar un diagrama:

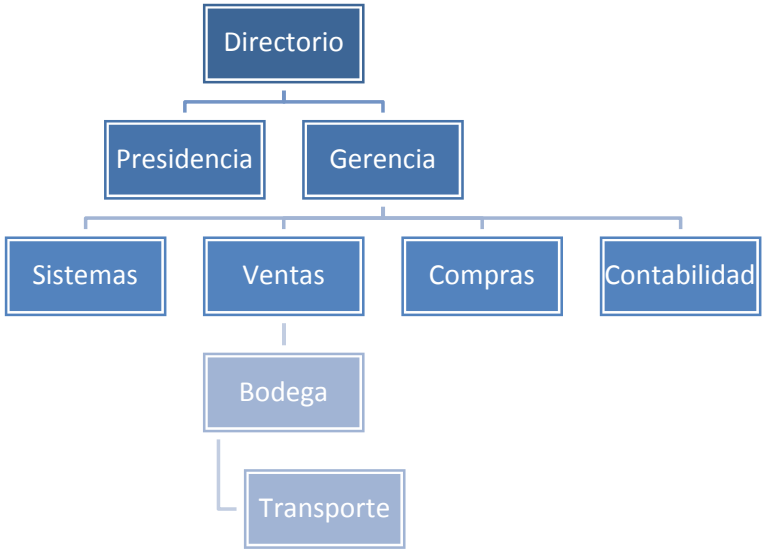


Grafico 9: Estructura Organizacional MADECO

Factores críticos de éxito / Procesos de Negocio	Nuevos Productos Competitivos	Empleados competentes	Satisfacción del Cliente	Valor Agregado: Calidad y Garantía	Imagen	TOTAL
Gestión Administrativa	X	X	X	X	X	5
Atención al Cliente		X	X	X	X	4
Compras Locales	X		X		X	3
Ventas		X	X		X	3
Entrega de pedidos		X	X		X	3
Almacenamiento de Mercadería		X	X		X	2
Adquirir e Implementar		X		X		2
Despacho de Mercadería		X	X			2
Control de Inventarios		X	X			2
Dirección y Control		X	X			2
Desarrollo, entrega y soporte		X	X			2
Gestión de RRHH		X	X		X	2
Auditoría y Control de procesos Críticos de Negocio			X		X	2
Coordinación Principal					X	1
Proceso Contable					X	1
Planificación y Organización de Proyectos			X			1

Tabla 9: Matriz de Despliegue (Nivicela)

Con el análisis resultante de la matriz de despliegue se llega a la conclusión de que los procesos críticos de negocio en los que se va a poner mayor énfasis dentro del Plan de Gestión de Riesgos de la Información y los procesos de apoyo de la empresa están distribuidos de la siguiente manera

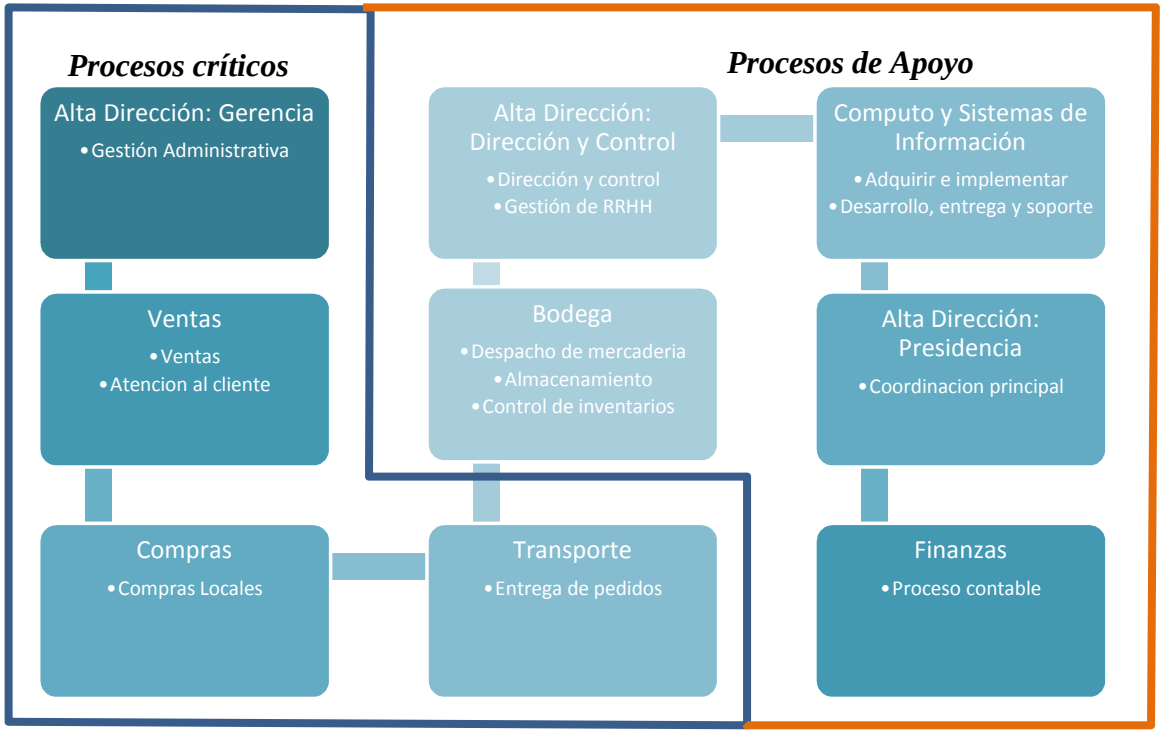


Grafico 10: Mapa de procesos de Negocio (Nivicela)

CAPITULO 3: ANALISIS DE ACTIVOS

En este capítulo se reconocerán los activos de información críticos de la empresa, mediante el levantamiento de información que incluyó revisión y comprobación de los puestos de trabajo, datos manejados por la organización, información de equipamiento físico y lógico, así como locales de la organización.

2.4. Identificación de activos de información

Los activos de información son aquellos que tienen valor para la organización, por tanto la esta debe protegerlos. (A. G. Gomez).

Esta afirmación nos lleva a reconocer los activos de información de alta prioridad para MADECO. Los mismos que forman parte del conjunto de procesos críticos de negocio reconocidos en el capítulo 2. Es por ello que se ha llevado a cabo el levantamiento de activos de información de los procesos de negocio críticos, los cuales han sido identificados gracias a la participación de los dueños de los procesos.

2.5. Análisis de activos a través de la Metodología MAGERIT v2

2.5.1. Clasificación de activos

La norma ISO 27001:2005 a través de MAGERIT v2 ha clasificado estos activos de acuerdo a su función:

[S]Servicios

- **[**anon**]** anónimo
- [pub] al público en general
- [ext] a usuarios externos
- [int] interno
- [cont] contratado a terceros
- [www] world wide web

- [telnet] acceso remoto o cuenta local
- [email] correo electrónico
- [file] almacenamiento de ficheros
- [ftp] transferencia de ficheros
- [edi] intercambio electrónico de datos
- [dir] servicio de directorio
- [idm] gestión de identidad
- [ipm] gestión de identidades
- [pki] PKI/infraestructura de clave publica

[D] Datos/Información

- **[**vr**]** datos vitales
- [com] datos de interés comercial
- [adm] datos de interés para la administración publica
- [int] datos de gestión interna
- [voice] voz
- [multimedia] multimedia
- [source] código fuente
- [exe] código ejecutable
- [conf] datos de configuración
- [log] registro de actividad
- [test] datos de prueba
- [per] datos de carácter personal

    - [A] de nivel alto
    - [M] de nivel medio
    - [B] de nivel básico
- [label] datos clasificados
    - [S] secreto
    - [R] reservado
    - [C] confidencial
    - [DL] difusión limitada
    - [SC] sin clasificar

[SW] Aplicaciones

- **[**prp] desarrollo propio
- [sub] desarrollo a medida
- [std] estándar
    - [browser] navegador web
    - [www] servidor de presentación
    - [app] servidor de aplicaciones
    - [email_client] cliente de correo electrónico
    - [file] servidor de ficheros
    - [dbms] sistema de gestión de base de datos
    - [tm] monitor transaccional
    - [office] ofimática
    - [av] anti virus
    - [os] sistema operativo

    - [ts] servidor de terminales
    - [backup] sistema de backup

[HW] Equipos informáticos

- [host] grandes equipos
- [mid] equipos medios
- [pc] informática personal
- [mobile] informática móvil
- [pda] agendas electrónicas
- [easy] fácilmente reemplazable
- [data] que almacena datos
- [peripheral] periféricos
    - [print] medios de impresión
    - [scan] escáneres
    - [crypto] dispositivos criptográficos
- [network] soporte de red
    - [modem] módems
    - [hub] concentradores
    - [switch] conmutadores
    - [router] encaminadores
    - [bridge] pasarelas
    - [firewall] cortafuegos
    - [wap] punto de acceso wireless
- [pabx] centralita telefónica

[COM] Redes de comunicaciones

- [PSTN] red telefónica
- [ISDN] rdsi
- [X25] X25
- [ADSL] ADSL
- [pp] punto a punto
- [radio] red inalámbrica
- [sat] por satélite
- [LAN] red local
- [MAN] red metropolitana
- [Internet] Internet
- [vpn] red privada virtual

[SI] Soportes de información

- [electronic] electrónicos
    - [disk] discos
    - [san] almacenamiento en red
    - [cd] CD-ROM
    - [usb] dispositivos USB
    - [dvd] DVD
    - [tape] cinta magnética
    - [mc] tarjetas de memoria
    - [ic] tarjetas inteligentes

- [non_electronics] no electrónicos
    - [printed] material impreso
    - [tape] cinta de papel
    - [film] microfilm
    - [cards] tarjetas perforadas

[AUX] Equipamiento auxiliar

- [power] fuentes de alimentación
- [ups] sistemas de alimentación ininterrumpida
- [gen] generadores eléctricos
- [ac] equipos de climatización
- [cabling] cableado
- [robot[] robots
    - [tape] de cintas
    - [disk] de discos
- [supply] suministros esenciales
- [destroy] equipos de destrucción de soportes de información
- [furniture] mobiliari: armarios, etc
- [safe] cajas fuertes

[L] Instalaciones

- [site] emplazamiento
- [buildIng.] edificio
- [local] local

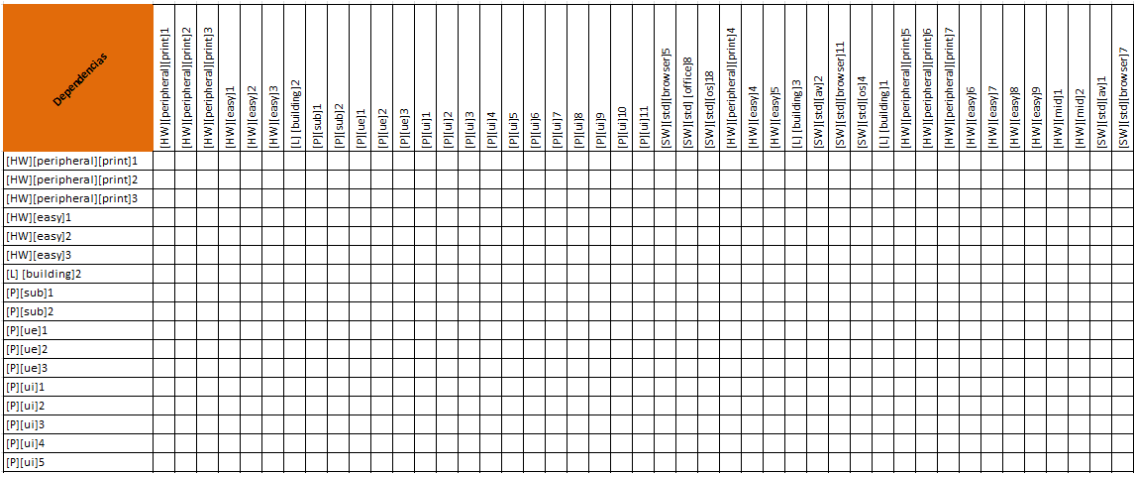
- [mobile] plataformas mobiles
    - [car] vehículo terrestre: coche, camión, etc
    - [plane] vehículo aéreo: avión, etc
    - [ship] vehículo marítimo: buque, lancha, etc
    - [shelter] contenedores
- [cannel] canalización

[P] Personal

- [ue] usuarios externos
- [ui] usuarios internos
- [op] operadores
- [adm] administradores de sistemas
- [com] administradores de comunicaciones
- [dba] Administradores de BBDD
- [des] desarrolladores
- [sub] subcontratas
- [prov] proveedores (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

2.5.2. Dependencias entre activos

Las dependencias entre activos permiten considerar activos que no están directamente relacionados con los procesos críticos, pero que impactan de igual manera a la integridad, disponibilidad y confidencialidad. *Ver cuadro completo anexo 8*



Dependencias	[HW][peripheral][print]1	[HW][peripheral][print]2	[HW][peripheral][print]3	[HW][easy]1	[HW][easy]2	[HW][easy]3	[L] [building]2	[P][sub]1	[P][sub]2	[P][ue]1	[P][ue]2	[P][ue]3	[P][ui]1	[P][ui]2	[P][ui]3	[P][ui]4	[P][ui]5	[P][ui]6	[P][ui]7	[P][ui]8	[P][ui]9	[P][ui]10	[P][ui]11	[SW][std][browser]5	[SW][std] [office]8	[SW][std][os]18	[HW][peripheral][print]4	[HW][easy]4	[HW][easy]5	[L] [building]3	[SW][std][av]2	[SW][std][browser]11	[SW][std][os]4	[L] [building]1	[HW][peripheral][print]5	[HW][peripheral][print]6	[HW][peripheral][print]7	[HW][easy]6	[HW][easy]7	[HW][easy]8	[HW][easy]9	[HW][mid]1	[HW][mid]2	[SW][std][av]1	[SW][std][browser]7
[HW][peripheral][print]1																																													
[HW][peripheral][print]2																																													
[HW][peripheral][print]3																																													
[HW][easy]1																																													
[HW][easy]2																																													
[HW][easy]3																																													
[L] [building]2																																													
[P][sub]1																																													
[P][sub]2																																													
[P][ue]1																																													
[P][ue]2																																													
[P][ue]3																																													
[P][ui]1																																													
[P][ui]2																																													
[P][ui]3																																													
[P][ui]4																																													
[P][ui]5																																													

Grafico 11: Matriz de dependencias entre activos

(Nivicela)

2.5.3. Valoración

Una vez culminado el reconocimiento de los activos de información, se va a proceder a realizar el modelo de valor, el mismo que consiste en valorar a los activos de información de acuerdo a las dimensiones de interés que propone la ISO 27001:2005 a través de MAGERIT.

2.5.4. Dimensiones de interés

Las dimensiones de interés hacen referencia a los tres pilares de la seguridad de la información: **Disponibilidad, integridad, confidencialidad**, y adicionalmente aspectos como la **validación del origen de usuarios** y de los **datos**, así como la **trazabilidad del servicio**.

Se van a analizar cuáles serían las consecuencias negativas para la PYME al prescindir de las dimensiones del modelo de valor propuesto por MAGERIT. Cada una de las dimensiones será valorada según los criterios descritos en las tablas en la parte inferior.

Según la escala de Likert del capítulo 1 (Graf. 4)

Valor		**Criterio**
1	Muy Bajo	Irrelevante
2	Bajo	Bajo
3	Medio	Medio
4	Alto	Alto
5	Muy Alto	Muy alto

Tabla 11: Escala Likert para valoración de activos (A. G. Gomez)

Para caracterizar a los activos según la escala de valoración, se va a tener las siguientes consideraciones:

VALOR	**CRITERIO**
1	Puede causar menor confianza dentro de la organización Puede afectar la seguridad de las personas Puede causar incidentes leves entre los implicados No supone daño a la imagen o integridad de la PYME o el personal
2	Puede causar daños menores a un individuo o grupo de individuos Puede llegar a impedirse parte de la operación de la PYME Puede afectar las relaciones internas de la organización
3	Afecta a un individuo o grupo de individuos Puede quebrantar la ley o reglamento de protección de información personal Puede causar manifestaciones o presiones significativas

4	Puede amenazar la vida de uno o más individuos Puede interrumpir la investigación de una situación determinada Puede causar inconvenientes en la relación cliente/vendedor
5	Puede causar interrupciones en el funcionamiento de la organización Puede significar pérdida de vidas humanas Puede causar alteración del orden publico Puede conllevar al cierre de la empresa Puede causar publicidad negativa Puede causar incumplimiento de una ley o regulación

Tabla 12: Escala Estándar minimizada para valoración de dimensiones de interés e impacto de amenazas
(Públicas)

2.5.5. Valoración Cuantitativa y cualitativa

MAGERIT sugiere dos tipos de valoración de activos:

Cuantitativo: Consideraciones numéricas precisas de la importancia de los activos para la empresa. Esta valoración incluye las dependencias entre activos. Siendo este método el más idóneo, se utilizara en este estudio.

Cualitativo: Nos ofrece una calificación subjetiva del valor de los activos.

2.5.6. Evaluación de daños con la pérdida o alteración de un activo

Al utilizar la valoración cuantitativa obtenemos cantidades que pueden ser usadas para ser combinadas con valores expresados en dinero ganado o dinero perdido para la empresa. El objetivo es indicar las pérdidas económicas que representarían la pérdida o alteración de un activo, frente a la inversión que se podría hacer en protección de los mismos. Esta calificación se llevara a cabo mediante la valoración de los propietarios de cada proceso al que corresponden los activos, serán ellos

mismos los encargados de determinar las consecuencias de alterar, perder o prescindir de la trazabilidad de un activo.

CAPITULO 4: ANALISIS DE AMENAZAS Y VULNERABILIDADES A TRAVES DE MAGERIT

4.1. Valoración de amenazas

Las amenazas son valoradas por la frecuencia y el impacto que se puede producir haciendo que un activo sea degradado. Cada amenaza afecta en mayor escala a un grupo de activos afectando su disponibilidad, confidencialidad e integridad. Para categorizar la frecuencia de ocurrencia nos basaremos en la siguiente tabla

Valor	**Descripción**	**Frecuencia**
1	Muy baja	Casi nunca
2	Baja	Anual
3	Media	Semestral
4	Alta	Mensual
5	Muy Alta	Diario

Tabla 13: Frecuencia de una amenaza (Nivicela)

Según la Metodología MAGERIT cada amenaza representa la degradación de un conjunto de activos y la pérdida de sus cualidades (disponibilidad, integridad, confidencialidad), por tanto, de acuerdo a la tabla siguiente se ha catalogado y calificado la frecuencia de ocurrencia sobre los activos de la organización que pueden ser afectados por la lista de amenazas descritas. Lo planteado puede verse en el Anexo 4

CODIGO	TIPO DE ACTIVO	DIMENSIONES
[N.1]FUEGO	[HW]Equipos informáticos	1. [D] Disponibilidad datos
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[L]Instalaciones	
[N.2] DANOS POR AGUA	[HW]Equipos informáticos	1. [D] Disponibilidad
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[L]Instalaciones	
[I.1] FUEGO	[HW]Equipos informáticos	1. [D] Disponibilidad
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[L]Instalaciones	
	[AUX] Equipamiento auxiliar	
[I.2] DANOS POR AGUA	[HW]Equipos informáticos	1. [D] Disponibilidad
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[L]Instalaciones	
	[AUX] Equipamiento auxiliar	
[I.*] DESASTRES INDUSTRIALES	[HW]Equipos informáticos	1. [D] Disponibilidad
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[L]Instalaciones	
[I.3] CONTAMINACION MECANICA	[AUX] Equipamiento auxiliar	1. [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	[AUX] Equipamiento auxiliar	1. [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[SW] Aplicaciones	
[I.6] CORTE DEL SUMINISTRO ELECTRICO	[AUX] Equipamiento auxiliar	1. [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD	[AUX] Equipamiento auxiliar	1. [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
[I.8]FALLO DEL SERVICIO DE COMUNICACIONES	[COM]Redes de comunicaciones	1. [D] Disponibilidad

[I.9] INTERRUPCION DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	[AUX] Equipamiento auxiliar	1. [D] Disponibilidad
[I.10] DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	[SI]Soportes de información	1. [D] Disponibilidad
[I.11] EMACIONES ELECTROMAGNETICAS	[HW]Equipos informáticos	1. [C] Confidencialidad
	[COM]Redes de comunicaciones	
	[L]Instalaciones	
[E.1] ERRORES DE LOS USUARIOS	[S] Servicios	1. [I] Integridad 2. [D] Disponibilidad
	[D] Datos	
	[SW] Aplicaciones	
[E.2] ERRORES DEL ADMINISTRADOR	[HW]Equipos informáticos	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
	[COM]Redes de comunicaciones	
	[S] Servicios	
	[D] Datos	
	[SW] Aplicaciones	
[E.3] ERRORES DE MONITORIZACION (LOG)	[S] Servicios	1. [I] Integridad 2. [C] Confidencialidad
	[D] Datos	
	[SW] Aplicaciones	
[E.4] ERRORES DE CONFIGURACIÓN	[S] Servicios	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
	[D] Datos	
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
[E.7] DEFICIENCIAS EN LA ORGANIZACIÓN	[P] Personal	1. [D] Disponibilidad
[E.8] DIFUSION DE SOFTWARE DANINO	[SW] Aplicaciones	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
[E.14] ESCAPES DE INFORMACIÓN	[D] Datos [SW] Aplicaciones	1. [C] Confidencialidad
	[COM]Redes de comunicaciones	

[E.16] INTRODUCCION DE INFORMACIÓN INCORRECTA	[D] Datos	1 [I] Integridad
[E. 17] DEGRADACION DE LA INFORMACIÓN	[D] Datos	1. [I] Integridad
[E.18] DESTRUCCION DE LA INFORMACIÓN	[D] Datos	1 [D] Disponibilidad
[E.19] DIVULGACION DE INFORMACIÓN	[D] Datos	1. [C] Confidencialidad
[E.20] VULNERABILIDADES DE LOS PROGRAMAS SOFTWARE	[SW] Aplicaciones	1. [I] Integridad 2. [D] Disponibilidad 3. [C] Confidencialidad
[E.21] ERRORES DE MANTENIMIENTO/ACTUALIZACION SOFTWARE	[SW] Aplicaciones	1. [I] Integridad 2. [D] Disponibilidad
[E.23] ERRORES DE MANTENIMIENTO/ACTUALIZACION HARDWARE	[HW]Equipos informáticos	1 [D] Disponibilidad
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[SW] Aplicaciones	1 [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
[E.28] INDISPONIBILIDAD DEL PERSONAL	[P] Personal	1 [D] Disponibilidad
[A.4] MANIPULACION DE LA CONFIGURACIÓN	[S] Servicios	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
	[D] Datos	
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
[A.5] SUPLANTACION DE IDENTIDAD DEL USUARIO	[S] Servicios	1. [I] Integridad 2. [C] Confidencialidad
	[SW] Aplicaciones	
	[COM]Redes de comunicaciones	
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	[S] Servicios	1. [D] Confidencialidad 2. [I] Integridad
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	

[A.7] USO NO PREVISTO	[S] Servicios	1 [D] Disponibilidad
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[AUX] Equipamiento auxiliar	
	[L]Instalaciones	
[A.8] DIFUSION DE SOFTWARE DANINO	[SW] Aplicaciones	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
[A.11] ACCESO NO AUTORIZADO	[S] Servicios	1. [D] Confidencialidad 2. [I] Integridad
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[AUX] Equipamiento auxiliar	
	[L]Instalaciones	
	[D] Datos	
[A.13] REPUDIO	[S] SERVICIOS	1. [I] Integridad
[A.14] INTERCEPTACION DE INFORMACIÓN	[D] Datos	1. [C] Confidencialidad
	[SW] Aplicaciones	
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
[A.15] MODIFICACION DE LA INFORMACIÓN	[D] Datos	1. [I] Integridad
[A.16] INTRODUCCION DE FALSA INFORMACIÓN	[D] Datos	1. [I] Integridad
[A.17] CORRUPCION DE LA INFORMACIÓN	[D] Datos	1. [I] Integridad
[A.18] DESTRUCCION DE LA INFORMACIÓN	[D] Datos	1. [D] Disponibilidad
[A.19] DIVULGACION DE INFORMACIÓN	[D] Datos	1. [C] Confidencialidad
[A.22] MANIPULACION DE PROGRAMAS	[SW] Aplicaciones	1. [D] Disponibilidad 2. [I] Integridad

		3. [C] Confidencialidad
[A.24] DENEGACION DE SERVICIO	[S] Servicios	1. [D] Disponibilidad
	[HW]Equipos informáticos	
	[COM]Redes de comunicaciones	
[A.25] ROBO	[HW]Equipos informáticos	1. [D] Confidencialidad 2. [C] Confidencialidad
	[COM]Redes de comunicaciones	
	[SI]Soportes de información	
	[AUX] Equipamiento auxiliar	
[A.26] ATAQUE DESTRUCTIVO	[HW]Equipos informáticos [COM]Redes de comunicaciones [SI]Soportes de información	1. [D] Confidencialidad 2. [C] Confidencialidad
	[AUX] Equipamiento auxiliar	
[A.28] INDISPONIBILIDAD DEL PERSONAL	[P] Personal	1. [D] Disponibilidad
[A.29] EXTORSION	[P] Personal	1. [C] Confidencialidad 2. [I] Integridad
[A.30] ING.ENIERIA SOCIAL	[P] Personal	1. [C] Confidencialidad 2. [I] Integridad

Tabla 14: Amenazas por activo (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

4.2. Determinación de Impacto de una amenaza

El impacto de las amenazas se calificó con la colaboración de las partes interesadas, mediante la técnica de la valoración Delphi. *Véase: Anexo 5*

Valoración Delphi

La valoración Delphi tiene por objetivo analizar las opiniones de un conjunto de personas interesadas dentro de un proyecto, en donde a través de un banco de preguntas y/o lista de ítems se aborda la problemática de un tema en específico para dar soluciones consensuadas. Debido a la naturaleza de este método se llegan a recoger opiniones variadas más confiables ya que los participantes no se ven sometidos a presiones grupales o dominantes durante el proceso. El proceso consiste

en reconocer el tema que se va a abordar y el grupo de participantes o partes interesadas que pueden aportar a la solución del problema, en donde inicialmente se hace un sondeo con preguntas abiertas que posteriormente son utilizadas para refinar la información y generar un segundo banco de preguntas para obtener respuestas cerradas que facilitan la interpretación. Con el refinamiento se estructura la información de forma ordenada, de manera que se la pueda presentar a los participantes para que puedan dar una segunda opinión acerca de los resultados hasta que finalmente se llegue a un punto de consenso entre las opiniones de todas las partes.

Según el artículo de la Revista Investigación Educativa existen instrumentos de recogida de datos como son: la jerarquización de los temas que aborda la problemática, valoraciones basadas en escalas numéricas definidas, comparaciones entre elementos de análisis, elección de los elementos más importantes, estimaciones cuantitativas sobre los elementos estudiados. (Piñeiro)

4.3. Identificación de vulnerabilidades

Alexander Gómez en su libro Diseño de Gestión de un Sistema de Seguridad de la Información sugiere una lista de vulnerabilidades que pueden ser consideradas, las mismas que mediante la valoración Delphi, se ha procurado retroalimentar para ajustar el sistema al entorno y a la realidad en la que se desenvuelve la organización.

El primer conjunto de vulnerabilidades consideradas se puede observar en el Capítulo 1: Vulnerabilidades de la presente tesis. La retroalimentación se puede observar en el anexo completo de la matriz de riesgos *Véase: Anexo 6*

4.4. Determinación de riesgos

Como indica MAGERIT, los riesgos se producen de la materialización de una amenaza sobre un activo, explotando la vulnerabilidad. Es por esto que se ha realizado un cuadro siguiente, en donde se especifica una lista de amenazas posibles, las mismas que he analizado de acuerdo al entorno en que se desarrolla la empresa y las sugerencias de algunos autores sobre el tema. Además las partes interesadas han retroalimentado este análisis mediante la técnica Delphi, aplicada dentro de este estudio.

CODIGO	TIPO ACTIVO	VULNERABILIDADES	RIESGO
[N.1]FUEGO	[HW]Equipos informáticos	Falta de un sistema contra incendios	Se produzca un incendio que acabe con los activos de información
	[COM]Redes de comunicaciones		
	[L]Instalaciones		
[N.2] DANOS POR AGUA	[HW]Equipos informáticos	Goteras	Corto circuito y fallas en los equipos
	[COM]Redes de comunicaciones		
[I.1] FUEGO	[HW]Equipos informáticos	Explosión de productos inflamables	Explosión que acabe con los activos
	[COM]Redes de comunicaciones		
[I.2] DANOS POR AGUA	[HW]Equipos informáticos	Fugas de agua por daños de cañería	Dañarse los equipos que estén en el piso
	[COM]Redes de comunicaciones	Llaves de agua abiertas	Cortocircuito
	[SI]Soportes de información		
	[L]Instalaciones	Derramar líquidos sobre los equipos	Cortocircuito
	[AUX] Equipamiento auxiliar		
[I.*] DESASTRES INDUSTRIALES	[HW]Equipos informáticos	Cortocircuito	Se queman los equipos conectados
	[COM]Redes de comunicaciones		
	[SI]Soportes de información	Accidente de trafico	Destrucción de la edificación
	[L]Instalaciones		
[I.3] CONTAMINACION MECANICA	[AUX] Equipamiento auxiliar	Polvo	Sobrecalentamiento de los equipos
	[HW]Equipos informáticos		Falla de unidades de trabajo

	[COM]Redes de comunicaciones	Comer a lado de los equipos	Derramar líquidos y que el equipo haga cortocircuito
	[SI]Soportes de información		Derramar comida y causar fallas por impedimento de manipulación del equipo
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	[AUX] Equipamiento auxiliar	Defectos de fabrica de los equipos	Equipos que no trabajen correctamente o no funcionen
	[HW]Equipos informáticos		
[I.6] CORTE DEL SUMINISTRO ELECTRICO	[AUX] Equipamiento auxiliar	Apagones por fallos del proveedor	Detención de los servicios de impresión y procesamiento
	[HW]Equipos informáticos		
	[COM]Redes de comunicaciones		
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD	[AUX] Equipamiento auxiliar	Calor excesivo producido por los equipos	Sobrecalentamiento de los equipos
	[HW]Equipos informáticos		
	[COM]Redes de comunicaciones		Deterioro de ciertos materiales de los equipos que provocan fallas en los mismos
	[SI]Soportes de información		
[I.8]FALLO DEL SERVICIO DE COMUNICACIONES	[COM]Redes de comunicaciones	Desconexión de un cable de red	Perdida de comunicación interna o con otras sucursales
		Caída del servicio del ISP	No se puede utilizar el internet

		Dispositivo de comunicaciones quemado	Perdida de comunicación interna o con otras sucursales
		Dispositivos de comunicación mal configurados	Perdida de cálida de conexión entre terminales
[I.9] INTERRUPCION DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	[AUX] Equipamiento auxiliar	Se termine el papel para la impresora	interrupción en la impresión
		Se termine la cinta de las impresoras matriciales	No puedan emitir facturas
		Se termine el tóner de las impresoras laser	Los documentos se impriman borrosos
[I.10] DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	[SI]Soportes de información	Falta de conservación de los soportes de información	Perdida de información
		Mala manipulación de los soportes	
[E.1] ERRORES DE LOS USUARIOS	[S] Servicios	Falta de capacitación a los usuarios	Inconsistencia de datos del sistema
	[D] Datos	Falta de robustez del sistema	Reportes basura
	[SW] Aplicaciones	Falta de políticas de confidencialidad de información	Conflictos internos
[E.2] ERRORES DEL ADMINISTRADOR	[HW]Equipos informáticos	Sobrecarga de trabajo	No se tienen registros actualizados
	[COM]Redes de comunicaciones		
	[S] Servicios	Falta de plantillas de registro	No se dispone de una plantilla para registrar incidentes o

			actividades de soporte
	[D] Datos	Falta de plan o políticas de registro de bitácoras	Problemas mayores generados por falta de revisiones continuas
	[SW] Aplicaciones		
[E.3] ERRORES DE MONITORIZACION (LOG)	[S] Servicios	Falta de mecanismos de monitoreo	Perdida de continuidad de servicios
	[D] Datos		Perdida de documentos importantes
	[SW] Aplicaciones		Pérdida de conocimiento de actividades de procesos
[E.4] ERRORES DE CONFIGURACIÓN	[S] Servicios	Falta de manuales de configuración	Fallas al imprimir
			Fallas al usar el sistema
	[D] Datos		No se pueden enviar o recibir correos
	[SW] Aplicaciones	Falta de políticas de uso de aplicaciones y de información	Fallas al realizar o recibir llamadas
	[HW]Equipos informáticos	Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	Abusos de privilegios de internet
[E.7] DEFICIENCIAS EN LA ORGANIZACIÓN	[P] Personal	Falta de capacitación sobre seguridad de la información	No se cumplan las políticas que salvaguardan la información
		Falta de mecanismos de monitoreo del personal	Retardo en el cumplimiento de procesos

		Falta de políticas de uso correcto de telecomunicaciones	Uso personal de los activos
		Falta de políticas de contratación	Negligencia
		Carencia de control en la entrega de activos al caducar el contrato	SGSI desactualizado
		Empleados desmotivados	Problemas con los clientes
[E.8] DIFUSION DE SOFTWARE DANINO	[SW] Aplicaciones	Falta de políticas de uso de aplicaciones y de información	Virus
		Falta de control sobre la seguridad de la red	Spam
			Rootkits
		Falta de herramientas de protección de los equipos de TI	Troyanos
[E.14] ESCAPES DE INFORMACIÓN	[D] Datos	Falta de capacitación sobre seguridad de la información	No se cumplan las políticas que salvaguardan la información
		Carencia de mecanismos que controlen el envió y recepción de mensajes	Intercepción y robo de información
	[SW] Aplicaciones	Falta de políticas de uso de aplicaciones y de información	Divulgación de información confidencial
	[COM]Redes de comunicaciones	Falta de control de acceso físico a oficinas o salones restringidos	Intrusos en áreas restringidas que pueden robar, sabotear o destruir los recursos de tratamiento de información

[E.16] INTRODUCCION DE INFORMACIÓN INCORRECTA	[D] Datos	Falta de concentración de los usuarios	Inconsistencia de datos del sistema
[E. 17] DEGRADACION DE LA INFORMACIÓN	[D] Datos	Carencia de planes de restitución de equipos	Perdida de respaldos de información valiosa
			Trunca el trabajo de los empleados que hacen uso del activo
		Ubicación de los recursos en espacios desprotegidos	Daños físicos del equipo por ende perdida de la información
			Robo del equipo y perdida de la información no respaldada
		Falta de control del uso y buen funcionamiento de los equipos	Daños internos del equipo que dificultan su operación
[E.18] DESTRUCCION DE LA INFORMACIÓN	[D] Datos	Falta de plan de respaldos de información critica	Perdida de disponibilidad de la información
[E.19] DIVULGACION DE INFORMACIÓN	[D] Datos	Falta de capacitación sobre seguridad de la información	No se cumplan las políticas que salvaguardan la información
		Carencia de control en la entrega de activos al caducar el contrato	Perdida de activos
			Desactualización del SGSI
[E.20] VULNERABILIDADES DE LOS	[SW] Aplicaciones	Mala administración de llaves criptográficas	Acceso no autorizado a información confidencial

PROGRAMAS SOFTWARE		Falta de validación de datos procesados	Inconsistencia de datos del sistema
		Mala estructuración de la base de datos	Funcionamiento parcial de la aplicación
		Falta de políticas de uso de aplicaciones e información	Perdida de seguridad
		Carencia de pruebas de software	Uso limitado de recursos aplicativos
[E.21] ERRORES DE MANTENIMIENTO/ACTUALIZACION SOFTWARE	[SW] Aplicaciones	Falta de planes de actualización	Aumento de vulnerabilidades software
		Software no licenciado	Uso limitado de características del aplicativo
		La aplicación desactivada para actualizaciones	Perdida de eficiencia y eficacia del aplicativo
		Falta de plan de mantenimiento	Obsolescencia
[E.23] ERRORES DE MANTENIMIENTO/ACTUALIZACION HARDWARE	[HW]Equipos informáticos	Falta de un plan de mantenimiento de equipos de TI	Obsolescencia
		Falta de plan de gestión y control de recursos vs requerimientos	Funcionamiento no acorde a los requerimientos actuales de entorno
		Falta de mantenimiento preventivo	Mal funcionamiento de los equipos
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[SW] Aplicaciones	Carencia de un plan de restitución de equipos	Caída de los servicios proporcionados
	[HW]Equipos informáticos		Pérdida de calidad de servicios proporcionados
	[COM]Redes de		

	comunicaciones		
[E.28] INDISPONIBILIDAD DEL PERSONAL	[P] Personal	Falta de políticas de contratación	Faltas injustificadas
		Falta de un plan de contingencia en caso de ausencia	Puesto vacío de trabajo
[A.4] MANIPULACION DE LA CONFIGURACIÓN	[S] Servicios	Segmentación de redes incorrecta	Denegación de servicio
			Caída del servicio
	[D] Datos	Falta de políticas de uso de aplicaciones y de información	Errores al ejecutar aplicaciones
			Uso inadecuado de activos
	[SW] Aplicaciones	Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	Datos no reconocidos por los sistemas
	[HW]Equipos informáticos	Gestión de red inadecuada	Fallos de conexión
			Limitación en el desempeño de los equipos
	[COM]Redes de comunicaciones	Carencia de control en envió y recepción de mensajes	Indisponibilidad del servicio de comunicación
			SPAM
		Falta de protección en redes públicas de conexión	Ataques Hacker, Cracker
			Alteración o robo de información
[A.5] SUPLANTACION DE IDENTIDAD DEL USUARIO	[S] Servicios	Falta de capacitación sobre seguridad de la información	Robo de información
			Alteración de información
	[SW] Aplicaciones	Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	Abuso de privilegios de acceso

	[COM]Redes de comunicaciones	Falta de protección en redes públicas de conexión	Ataques Hacker, Cracker
			Robo o alteración de información
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	[S] Servicios	Gestión de red inadecuada	Robo de información
	[SW] Aplicaciones		Alteración de información
	[HW]Equipos informáticos		Hacking., Cracking., Pishing.
[A.7] USO NO PREVISTO	[S] Servicios	Falta de mecanismos de monitoreo del personal	Alteración de información
	[SW] Aplicaciones		Indisponibilidad de recursos lógicos o físicos
	[HW]Equipos informáticos		
	[SI]Soportes de información	Falta de políticas de uso correcto de telecomunicaciones	Desempeño bajo de los equipos y aplicaciones
	[AUX] Equipamiento auxiliar		Uso personal de los activos
[A.8] DIFUSION DE SOFTWARE DANINO	[SW] Aplicaciones	Gestión de red inadecuada	Denegación de servicio
			Ralentización de los servicios a través de la red
		Falta de políticas de protección al equipo de TI	Virus, Troyanos, Rootkits
[A.11] ACCESO NO AUTORIZADO	[S] Servicios	Gestión de red inadecuada	Modificaciones de información
	[SW] Aplicaciones		Robo de información
	[D] Datos		Destrucción de información, des configuración de aplicativos

[A.13] REPUDIO	[S] SERVICIOS	Carencia de mecanismos que controlen el envió y recepción de mensajes	Conflictos legales por no recepción de mensajes
			Conflictos por no recibir notificaciones o información solicitada
[A.14] INTERCEPTACION DE INFORMACIÓN	[D] Datos	Carencia de mecanismos que controlen el envió y recepción de mensajes	Robo de información
	[SW] Aplicaciones	Gestión de red inadecuada	Modificaciones de información
	[HW]Equipos informáticos	Falta de protección en redes públicas de conexión	Destrucción de la información
[A.15] MODIFICACION DE LA INFORMACIÓN	[D] Datos	Carencia de políticas de seguridad de uso de soportes de información externos	Mala publicidad
[A.16] INTRODUCCION DE FALSA INFORMACIÓN	[D] Datos	Carencia de políticas de seguridad de uso de soportes de información externos	Mala publicidad
			Reclamos por inconsistencias
[A.17] CORRUPCION DE LA INFORMACIÓN	[D] Datos	Carencia de políticas de seguridad de uso de soportes de información externos	Pérdida de credibilidad de la empresa
			Reclamos por inconsistencias
[A.18] DESTRUCCION DE LA INFORMACIÓN	[D] Datos	Carencia de políticas de seguridad de uso de soportes de información externos	Indisponibilidad de información a la mano
			Perdida de información
[A.19]	[D] Datos	Empleados desmotivados	Mayor competencia

DIVULGACION DE INFORMACIÓN		Falta de mecanismos de monitoreo	Mala publicidad
		Falta de capacitación sobre seguridad de la información	Mala publicidad
[A.22] MANIPULACION DE PROGRAMAS	[SW] Aplicaciones	Falta de políticas de uso de aplicaciones y de información	Des configuración de aplicaciones
			Fallas al ejecutar aplicaciones
		Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	Intentos de configuración sin autorización
[A.24] DENEGACION DE SERVICIO	[S] Servicios	Uso complicado de interfaces	Retraso en el procesamiento de información
	[HW]Equipos informáticos	Gestión de red inadecuada	Retraso en el cumplimiento de actividades del empleado
	[COM]Redes de comunicaciones	Carencia de planes de restitución de equipos	Perdida de continuidad de servicios
[A.25] ROBO	[HW]Equipos informáticos	Falta de control de acceso físico a oficinas o salones restringidos	Extracción de equipos de procesamiento de información
	[COM]Redes de comunicaciones	Ubicación de los recursos en espacios desprotegidos	Daños materiales a la organización
			Paralización parcial de funciones
	[SI]Soportes de información		Perdida económica
		Falta de control de uso y buen funcionamiento de los equipos	Perdida de información vital para la empresa
	[AUX] Equipamiento		

	auxiliar		
[A.26] ATAQUE DESTRUCTIVO	[HW]Equipos informáticos	Empleados desmotivados	Daños a los equipos de la organización
	[COM]Redes de comunicaciones	Conflictos civiles	Paralización parcial de funciones
			Perdidas económicas
	[SI]Soportes de información	Huelgas	Paralización parcial de funciones
	[AUX] Equipamiento auxiliar		Perdidas económicas
[A.28] INDISPONIBILIDAD DEL PERSONAL	[P] Personal	Falta de políticas de contratación	Actividades definidas incumplidas
			Retraso en el cumplimiento de actividades del empleado
			Retraso en la gestión de solicitudes del resto del personal
[A.29] EXTORSION	[P] Personal	Empleados desmotivados	Conflictos internos
			Mala publicidad
			Problemas Legales
[A.30] ING.ENIERIA SOCIAL	[P] Personal	Falta de capacitación sobre seguridad de la información	Robo de claves personales
			Acceso a áreas restrIng.idas
			Modificación o alteración de contenidos vitales
		Falta de mecanismos de monitoreo	Robo de información
			Empleados proporcionan información confidencial a

			personas no autorizadas
		Falta de políticas de uso correcto de telecomunicaciones	Personal emite datos confidenciales de la empresa por medios no seguros
			Personal no aplica criptografía y uso de claves de encriptación
		Empleados desmotivados	Empleados proporcionan claves de sistema y otros accesos voluntariamente
			Quejas del empleado en el Ministerio de Relaciones Laborales

Tabla 15: Tabla de riesgos (Nivicela)

CAPITULO 5: GESTIÓN DE RIESGOS CON MAGERIT

5.1. Evaluación de niveles de impacto y Riesgo Residual

El valor de la medición del riesgo se obtuvo a través de la fórmula propuesta por Alexander Gómez (VÉASE TABLA 5, PÁG. 27) en una matriz de amenazas sobre activos, donde se propone considerar el impacto que causaría la pérdida de un activo y la probabilidad de que la amenaza perjudique la estabilidad de estos activos.

Para poder entender y categorizar la importancia de los riesgos se consideró la siguiente tabla:

Valor	**Descripción**	**Riesgo**
0-5	Muy bajo	
6-10	Bajo	
11-15	Medio	
16-20	Alto	
21-25	Muy Alto	

Tabla 16: Impacto del riesgo (Nivicela)

Con base en el presente grafico podemos una lista priorizada de riesgos, donde se decidirá las acciones que se deberán tomar para mitigar, controlar o evitar el riesgo

Los riesgos serán contrarrestados de la siguiente manera

Riesgo	Acción
	Medidas de seguridad activas de prevención y detección
	Medidas de seguridad activas de prevención y detección
	Medidas de seguridad activas de prevención y detección
	Medidas de seguridad pasivas o de corrección
	Medidas de seguridad pasivas o de corrección

Tabla 17: Estrategias de Tratamiento de Riesgo
(Nivicela)

5.2. Determinar métodos de salvaguarda

Una vez culminado el análisis de los riesgos y habiendo reconocido cual será la estrategia de tratamiento del riesgo, se procede a determinar cuáles serán las mejores opciones activas de prevención y detección del riesgo. Para esta estrategia se dispone de dos medidas: mitigar y controlar. Estas medidas se van a aplicar mediante el uso de políticas de seguridad, sugerencias de capacitación e inducción al Sistema de Seguridad de Información, control de salvaguardas y procedimientos de recuperación ante riesgos suscitados. (Areitio)

5.2.1. **Métodos técnicos**

El objetivo de la aplicación de estas salvaguardas es contrarrestar las amenazas de origen lógico, como robo de datos y de información, interceptación de líneas de comunicación, sabotajes, virus, abuso de privilegios, accesos no autorizados, introducción de datos incorrectos, etc.

Para proteger estos recursos se van a utilizar las siguientes salvaguardas

1. **Protección de datos**
    a. Organización
        i. Clasificación de documentos:
            1. Por actividades desarrolladas-Orden Cronológico
            2. Por tipo de archivo-Por orden alfabético

b. Protección de valor
    i. Control de acceso:
        1. Acceso con claves personales
        2. Acceso por medio de huellas, retina, voz.
        3. Acceso mediante tarjetas personales
    ii. Firma electrónica
        1. Adquisición de firma electrónica
    iii. Copias de respaldo
        1. Plan de respaldos
        2. Rentar un espacio en la nube para realizar respaldos
        3. Adquisición de dispositivos externos para respaldo y planificación de traslado de respaldos.
    iv. Detección y recuperación
        1. Sistema de respaldos y plan de punto de restauración
    v. Cifrado de datos:
        1. Instalación de software para encriptación
        2. Implementación de código fuente de cifrado simétrico
    vi. Monitoreo
        1. Monitores transaccionales o instalación de aplicativos de monitoreo de red (Heredero, López y Martin-Romo)

2. Protección de Software

a. Ciclo de vida
    i. Protección código fuente
        1. Encriptación de código
    ii. Aceptación y puesta en operación
        1. Plan de pruebas
    iii. Gestión de cambios y configuración
        1. Plan de Control de Cambios
    iv. Gestión de incidencias
        1. Bitácora de mantenimiento correctivo
    v. Control de calidad
        1. Uso de estándares de desarrollo
        2. Planificación de proyectos
        3. Uso de estándares de medición de calidad de software
b. Protección de valor
    i. Protección frente a código dañino
        1. Implementación de antivirus
        2. Bloqueo de puertos de acceso a los equipos
        3. Gestión y control de navegación y descarga de contenido en internet

3. **Protección de las comunicaciones**
    a. Ciclo de vida
        i. Planificación de capacidad
            1. Uso de las normas internacionales ISOTEC 11801 y EIA/TIA 586 CSA (Castillo)
            2. Uso y aplicación de herramientas como PMBOOK para planificación de proyectos.
        ii. Adquisición y mantenimiento
            1. Plan de adquisición
            2. Plan de mantenimiento de redes y equipos de comunicación
            3. Plan de reposición de insumos de red
        iii. Segmentación de redes
            1. Diagramas de segmentación e infraestructura de redes
        iv. Configuración de routers
            1. Manuales de configuración de dispositivos
        v. Configuración de cortafuegos
            1. Manuales de configuración de dispositivos
        vi. Monitorización de ataques
            1. Aplicaciones de monitorización de actividades en tiempo real de la red
    b. Protección del valor
        i. Garantías de integridad
            1. Procedimientos para la protección y mantenimiento de equipos de comunicación
        ii. Cifrado
            1. Implementación software de cifrado de redes
        iii. Monitorización de actividades
            1. Monitorización periódica de actividades en los logs de los servidores.

        (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

5.2.2. **Métodos físicos**

Las salvaguardas que van a aplicarse se ajustan al entorno en el que se desarrolla la organización, contiene recomendaciones de uso de sistemas contra incendios, control de acceso a áreas restrIng.idas y a cualquier amenaza materializada que pueda interrumpir el funcionamiento normal de las localidades.

Para este control se han considerado las siguientes salvaguardas:

1. **Protección frente a amenazas naturales**
    a. Incendios:
        i. Extintores contra incendios
    b. Inundación:
        i. Piso falso
        ii. Filtradores de agua
        iii. Soporte/Base con ruedas para Case
2. **Protección frente a accidentes industriales**
    a. Incendio
        i. Extintores de incendios
    b. Contaminación mecánica:
        i. Sopletes
        ii. Limpiadores internos de precisión
3. **Protección de las edificaciones**
    a. Anuncios restrictivos:
        i. Avisos y señalización de privilegios de acceso
    b. Barreras físicas
        i. Puertas cerradas con llave
        ii. Dispositivos biométricos de acceso
    c. Protección de cableado
        i. Bandejas portacables
        ii. Canaletas de superficie
        iii. Tubos corrugados
4. **Control de acceso:**
    a. Personas:
        i. Dispositivos biométricos
        ii. Video vigilancia
    b. Equipos
        i. Video vigilancia
        ii. Candados
    c. Soportes de información
        i. Uso de archivos encriptados con claves personales

(Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

5.2.3. Medidas de control

Existen algunos aspectos de la organización que deben ser controlados para evitar caer en **amenazas asociadas con el personal** sobre errores de los usuarios, administración negligente, deficiencias en la organización, indisponibilidad del personal, extorsión y que los mismos puedan ser víctimas de Ing.eniería social.

1. Definición de perfiles para puestos de trabajo
    a. Elaboración de un perfil de trabajo por cada cargo
2. Selección del personal
    a. Control de cumplimiento de perfil laboral
3. Inducción a la seguridad de la información
    a. Procedimiento de inducción al nuevo contrata
    b. Entrega de folleto con el plan de seguridad
4. Formación continua
    a. Cronograma de capacitación de nuevas implementaciones para asegurar la Seguridad de la Información (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

Medidas de control para la contratación de servicios externos

1. SLA: Compromiso de disponibilidad de servicio
2. NDA: Compromiso de confidencialidad
3. Control de calificación de proveedores de servicios
4. Procedimientos de soporte para resolución de incidencias
5. Procedimiento de cierres de contrato
6. Procedimientos de penalización por incumplimiento de responsabilidades (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II)

Para todos los anteriores se requiere de la elaboración de un contrato con cada proveedor de servicio en donde se plasmen aspectos de confidencialidad, disponibilidad, responsabilidades y obligaciones del contratista y del contratante, sanciones por incumplimiento de ambas partes y cláusulas de cierre del contrato.

Por controles no únicamente se entienden los referentes al personal y a terceras partes externas, sino también al control de cumplimiento de las salvaguardas físicas y técnicas previamente expuestas. Así la norma ISO 27001 propone el siguiente modelo de control.

Objetivo de control	**Control**	**Aplicabilidad** ☐ SI ☐ NO	**Justificación**
A.5.1: Política de Seguridad de la Información	A.5.1.1	☒ SI ☐ NO	La organización carece de un SGSI, pero requiere de su implementación
	A.5.1.2	☒ SI ☐ NO	El crecimiento de la organizaciones una de sus metas, por tanto la variabilidad de activos y por consecuencia de su tratamiento.
A.6.1: Organización Interna	A.6.1.1	☒ SI ☐ NO	Sin el apoyo de la Alta Dirección, no se pueden aplicar muchos de los controles y además se requiere de inversión económica
	A.6.1.2	☒ SI ☐ NO	La organización se compone de varias áreas de negocio, tanto críticas como de apoyo, pero cada una de ellas proporciona recursos al sistema principal, por ende también deben considerarse dentro del proyecto
	A.6.1.3	☒ SI ☐ NO	Son varios los procesos y el departamento de TI dispone de pocas horas para atender y controlar a toda la organización. Además de que geográficamente las edificaciones de la organización están distantes entre ellas.
	A.6.1.4	☒ SI ☐ NO	Las decisiones que se tomen serán de gran impacto para la

			organización por tanto la Alta Dirección debe estar al tanto de todas las actividades que refieran a la implementación, mejora y monitorización del SGSI
	A.6.1.5	☐ SI ☒ NO	No aplica porque el único proceso que cumple la organización es la de vender. No existe una receta secreta que proteger.
	A.6.1.6	☐ SI ☒ NO	No se requiere de un control tan riguroso por tratarse de una organización con fines comerciales y cuya administración no es algo innovador.
	A.6.1.7	☒ SI ☐ NO	Es de gran importancia para el mejoramiento de un SGSI tener la opinión de personas entendidas y especializadas en este tema.
	A.6.1.8	☒ SI ☐ NO	El objetivo de la implementación de este sistema de Gestión de Riesgos es mantener a la organización protegida en tiempo real de los riesgos que se puedan suscitar, por ende se debe controlar que el sistema se encuentre actualizado y que se estén cumpliendo las políticas, controles y procedimientos de seguridad.
A.6.2:Partes externas	A.6.2.1	☒ SI ☐ NO	Dado que el personal de la organización tiene acceso externo hacia los sistemas internos, se debe controlar que solo personas autorizadas puedan hacer uso del mismo

			para evitar intrusiones no deseadas
	A.6.2.2	☐ SI ☒ NO	No aplica porque los clientes no acceden a nIng.una instancia del sistema de la organización que no sea únicamente el que proporcionan los empleados de atención al cliente.
	A.6.2.3	☒ SI ☐ NO	Aplica debido a que los servicios de tecnología de Información son proveídos por una empresa externa por ende hay riesgo de una brecha de seguridad.
A.7.1: Responsabilidad por lo activos	A.7.1.1	☒ SI ☐ NO	Debido al crecimiento de la organización, los activos rotan o se incrementan, por ende se debe mantener un inventario actualizado de los activos y su nivel de criticidad
	A.7.1.2	☒ SI ☐ NO	Los activos siempre deben estar asociados a un propietario que conozca la importancia del activo que maneja para poder incluirlo dentro del SGSI
	A.7.1.3	☒ SI ☐ NO	Uno de los aspectos que se tiene que considerar es que si no se tiene apoyo de los usuarios, no se puede cuidar de la seguridad de los activos. Por ende el control de educación del personal en el buen uso y cuidado de los activos a su cargo es muy importante
A.7.2: Clasificación de la información	A.7.2.1	☒ SI ☐ NO	Debido a que la empresa es un organismo comercial, está sujeto a leyes y reglamentaciones. Por eso la organización de la información es muy importante para tener

			en orden el ejercicio fiscal de la empresa.
	A.7.2.2	☒ SI ☐ NO	Una manera muy efectiva de llevar el control de documentos es que estos sean etiquetados de acuerdo a la importancia, actividades a las que se refiere, cronología de las mismas, etc. Con esto se facilita la búsqueda y seguimiento de ciertos procesos en los que la organización puede estar interesada.
A.8.1: Antes del empleo	A.8.1.1	☒ SI ☐ NO	Es conveniente que la organización mantenga un perfil definido para cada cargo con detalles de las obligaciones y responsabilidades con el objetivo de llevar adelante una empresa competente.
	A.8.1.2	☒ SI ☐ NO	La selección de aspirantes permite la contratación de la persona más idónea con un perfil más acercado a los requerimientos del puesto que se esté sorteando.
	A.8.1.3	☒ SI ☐ NO	El Ministerio de Relaciones Laborales exige la documentación de contratos en los que consten términos y condiciones del empleador hacia el empleado.
A.8.2:Durante el empleo	A.8.2.1	☒ SI ☐ NO	Es necesario plasmar as obligaciones de los activos durante el periodo de empleo
	A.8.2.2	☒ SI ☐ NO	Un Plan de Gestión de Riesgos Optimo se consigue con la colaboración de todo el personal. Con mayor razón si la empresa tiene planes de

			crecimiento dentro de sus metas.
	A.8.2.3	☒ SI ☐ NO	Si no se sanciona el incumplimiento de políticas y procedimientos de seguridad el Plan es inválido.
A.8.3: Terminación o cambio de empleo	A.8.3.1	☒ SI ☐ NO	Se deben acatar las normativas expuestas por el Ministerio de Relaciones Laborales para el finiquito del contrato (Ecuatoriana)
	A.8.3.2	☒ SI ☐ NO	Para evitar inconvenientes con el personal saliente y entrante y mantener en orden el inventario de activos y sus asignaciones
	A.8.3.3	☒ SI ☐ NO	Evitar riesgos de seguridad de acceso con los ex empleados
A.9.1: Áreas seguras	A.9.1.1	☒ SI ☐ NO	El área de Procesamiento de Información se encuentra desprotegida, no es un lugar apropiado para las instalaciones de Centro de Datos.
	A.9.1.2	☒ SI ☐ NO	El acceso al Área de Procesamiento de Información no está protegida contra robo o intrusión
	A.9.1.3	☒ SI ☐ NO	Los activos se encuentran desprotegidos contra robo, sobre todo los activos dedicados a la atención al público.
	A.9.1.4	☒ SI ☐ NO	Se disponen de sistemas contra incendios menores pero se debe controlar que en caso de emergencia estos equipos estén en buenas condiciones.
	A.9.1.5	☒ SI ☐ NO	Exigencias del Ministerio de Relaciones Laborales

			Resolución CD. 333. (Laborales)
	A.9.1.6	☒ SI ☐ NO	El área se encuentra aislada del acceso al público, pero no se tienen las seguridades necesarias para un Área de Procesamiento de Información.
A.9.2: Seguridad de los equipos	A.9.2.1	☒ SI ☐ NO	No todos los equipos tienen las protecciones debidas para evitar riesgos de perdida por desastres naturales, provocados o robos.
	A.9.2.2	☒ SI ☐ NO	El proceso de ventas y despacho de mercadería depende exclusivamente del Sistema y de los equipos de procesamiento de información.
	A.9.2.3	☒ SI ☐ NO	No se tiene cableado estructurado. La instalación de cableado corre peligro.
	A.9.2.4	☒ SI ☐ NO	No se dispone de un plan de mantenimiento preventivo de equipos de cómputo.
	A.9.2.5	☐ SI ☒ NO	Los activos de la organización no se movilizan
	A.9.2.6	☒ SI ☐ NO	Existe software de ofimática, sistema operativo y antivirus que se encuentra sin licenciamiento
	A.9.2.7	☐ SI ☒ NO	No se posee equipos portátiles que puedan ser extraídos.
A.10.1: Procedimientos y responsabilidades de operación	A.10.1.1	☒ SI ☐ NO	No se dispone de un manual de procedimientos operativos para los empleados.
	A.10.1.2	☒ SI ☐ NO	No se posee un control de gestión de cambios y se requiere como documentación

			según exigencias de la norma.
	A.10.1.3	☒ SI ☐ NO	El personal se encuentra desempeñando diferentes funciones, algunas de ellas vinculadas con procesos complementarios que pueden dar lugar a un fraude o error no controlado.
	A.10.1.4	☒ SI ☐ NO	Se posee un plan de desarrollo y pruebas no formalizado, pero no tiene un área de pruebas preproducción para evitar vulnerabilidades del sistema ya en producción.
A.10.2. Gestión de servicios de entrega de tercera parte	A.10.2.1	☒ SI ☐ NO	No se dispone de un contrato legal actualizado que respalde la entrega de servicio.
	A.10.2.2	☒ SI ☐ NO	Las actividades son controladas a un nivel no formal. No se realizan auditorías al proveedor
	A.10.2.3	☐ SI ☒ NO	El proveedor de servicio se vincula con todo el Sistema de Información así que está contemplado dentro de los procedimientos internos, con controles para servicios externos.
A.10.3: Planificación y aceptación del sistema	A.10.3.1	☒ SI ☐ NO	Existe un plan de gestión de capacidad no formalizado
	A.10.3.2	☐ SI ☒ NO	Contemplado dentro de A.10.3.1
A.10.4: Protección contra código malicioso y movible	A.10.4.1	☒ SI ☐ NO	Algunos de los equipos se encuentran sin nIng.ún aplicativo antivirus o de protección para el equipo. Los usuarios no están concientizados sobre los riesgos de seguridad que

			pueden provocar.
	A.10.4.2	☒ SI ☐ NO	Algunos de los equipos se encuentran sin nIng.ún aplicativo antivirus o de protección para el equipo. Los usuarios no están concientizados sobre los riesgos de seguridad que pueden provocar.
A.10.5: Copia de seguridad	A.10.5.1	☒ SI ☐ NO	No se tiene un plan de Backups para usuarios. No se dispone de un plan de Backups para los equipos de Base de Datos. No se dispone de equipamiento para la realización de Backups No se dispone de un plan de Backups para configuración de servidores.
A.10.6: Gestión de seguridad de la red	A.10.6.1	☒ SI ☐ NO	Se dispone de equipos para controlar la seguridad de la red pero no están monitoreadas y no se dispone de un plan para actualización de seguridad del mismo.
	A.10.6.2	☒ SI ☐ NO	No se dispone de una documentación de los servicios de red y niveles de entrega de servicio que requiere la empresa.
A.10.7: Manejo de medios de información	A.10.7.1	☐ SI ☒ NO	Se manejan con recursos compartidos en red.
	A.10.7.2	☐ SI ☒ NO	No se manejan medios removibles
	A.10.7.3	☒ SI ☐ NO	No existe un procedimiento formal que asegure el tratamiento de la información

	A.10.7.4	☒ SI ☐ NO	No están protegidos los accesos a la información
A.10.8: Intercambio de información	A.10.8.1	☒ SI ☐ NO	Tramite en línea de SRI, pagos en línea, estados de cuenta.
	A.10.8.2	☐ SI ☒ NO	No existe intercambio de información con entidades externas
	A.10.8.3	☒ SI ☐ NO	No existe traslado de medios de información, pero se va a recomendar para el plan de Backups.
	A.10.8.4	☒ SI ☐ NO	Los correos incluyen archivos de carácter confidencial y no existe una política de seguridad que regule este medio
	A.10.8.5	☒ SI ☐ NO	Las políticas se entregaran a la organización, pero ellos deberán encargarse de implementar el Sistema
A.10.9: Servicios de comercio electrónico	A.10.9.1	☐ SI ☒ NO	No se realiza comercio electrónico
	A.10.9.2	☐ SI ☒ NO	No se dispone de un sitio web de transacciones en línea
	A.10.9.3	☒ SI ☐ NO	Se dispone de un sitio web informativo para conocimiento de clientes (precios, productos)
A.10.10: Seguimiento	A.10.10.1	☒ SI ☐ NO	Requisito de la norma ISO 27001 para el seguimiento del cumplimiento del SGSI y mejoramiento del Plan de Gestión de Riesgos
	A.10.10.2	☒ SI ☐ NO	Es importante la trazabilidad de manipulación de información (facturas mal Ing.resadas, inventarios incorrectos, carteras invalidas, facturas mal emitidas)

	A.10.10.3	☒ SI ☐ NO	Los registros serán únicamente de dominio del personal de TI autorizado y de la Alta Dirección
	A.10.10.4	☒ SI ☐ NO	Si algún cambio falla se puede volver a un estado anterior quitanto los cambios actuales
	A.10.10.5	☒ SI ☐ NO	Aportar para futuros problemas del mismo tipo y poder actual instantáneamente. Aporta para el plan de gestión de riesgos
	A.10.10.6	☒ SI ☐ NO	Consistencia de cuadres de caja al final la jornada.
A.11.1:Requisitos del negocio para el control de accesos	A.11.1.1	☒ SI ☐ NO	Se va a establecer una política de control de accesos para el Centro de Procesamiento de la Información y para la seguridad de los usuarios y equipos.
A.11.2: Gestión de acceso a usuarios	A.11.2.1	☒ SI ☐ NO	Cuando finiquite el contrato todos los permisos del usuario puedan ser revocados sin dejar brechas de seguridad.
	A.11.2.2	☒ SI ☐ NO	Actualmente se controla pero no a un nivel formal. Pero es necesario conocer los privilegios de acceso para llevar un control estricto.
	A.11.2.3	☒ SI ☐ NO	Las claves son de dominio personal y de los administradores del sistema. Las claves del correo y mensajería son administradas por los mismos usuarios.
	A.11.2.4	☐ SI ☒ NO	El Gerente es el encargado de autorizar los accesos que el empleado necesita al iniciar sus labores dentro de la empresa

A.11.3: Responsabilidades de usuarios	A.11.3.1	☒ SI ☐ NO	Los usuarios son inconscientes de lo sensibles que pueden ser las claves
	A.11.3.2	☒ SI ☐ NO	En el área de atención al cliente los usuarios dejan desentendidas sus estaciones de trabajo y el área de sus estaciones de trabajo es accesible por tratarse de las ventas.
	A.11.3.3	☒ SI ☐ NO	Los usuarios tienen facturas, retenciones, órdenes de entrega sobre sus escritorios. Los usuarios mantienen gran parte de sus archivos en los escritorios de sus pantallas.
A.11.4: Control de acceso a la red	A.11.4.1	☒ SI ☐ NO	El personal trabaja con la compartición de recursos en red
	A.11.4.2	☒ SI ☐ NO	Se utilizan los accesos remotos para dar soporte al usuario.
	A.11.4.3	☒ SI ☐ NO	Cualquier PC que logre tener una conexión con la red tiene acceso al sistema, dado que la plataforma del sistema es Web.
	A.11.4.4	☒ SI ☐ NO	La utilización de aplicaciones para conexiones remotas deja puertos abiertos que pueden ser atacados por hackers
	A.11.4.5	☒ SI ☐ NO	Se comparte el servicio de internet a través de Wifi con Direcciónes pertenecientes a la misma red de trabajo.
	A.11.4.6	☒ SI ☐ NO	Actualmente se tienen la red segregada, pero en futuros proyectos se debe considerar la misma solución a un nivel formalizado.

	A.11.4.7	☐ SI ☒ NO	El acceso a la red Wifi no se encuentra vinculada con la red interna que maneja el sistema.
A.11.5: Control de acceso al Sistema Operativo	A.11.5.1	☒ SI ☐ NO	Para acceder a los equipos se requiere de una contraseña. Se mantiene un control, pero no a nivel formal.
	A.11.5.2	☐ SI ☒ NO	Existen dos grupos de usuarios: Administración interna y ventas. El primer grupo dispone de equipos personales por ende el uso único de contraseñas es válido. El segundo grupo es el personal de ventas que básicamente comparten las computadoras pero no tienen información de mayor valor, más que el sistema. Pero el Sistema Comercial tiene sus propios accesos.
	A.11.5.3	☐ SI ☒ NO	Las contraseñas serán manejadas a nivel de usuario, la gestión de seguridad de los mismos radica en la concientización del personal
	A.11.5.4	☒ SI ☐ NO	Falta de control sobre las aplicaciones que pueden instalar los usuarios no administradores
	A.11.5.5	☒ SI ☐ NO	Brecha de seguridad sobre los equipos que no estén atendidos y con sesiones abiertas.
	A.11.5.6	☒ SI ☐ NO	Cuentas de usuarios activas 24 horas
A.11.6: Control de acceso a las aplicaciones de información	A.11.6.1	☒ SI ☐ NO	Las aplicaciones de antivirus y red son de configurables a nivel de usuario operador.
	A.11.6.2	☐SI ☒ NO	La única aplicación crítica que

			manejan los usuarios operadores es el navegador para poder acceder al sistema y al correo, no es necesario aislar la aplicación. No hay inconveniente con la aislación de antivirus o aplicaciones de ofimática porque son de uso general.
A.11.7: Computación móvil y trabajo a distancia	A.11.7.1	☒ SI ☐ NO	Las personas que conforman la Alta Dirección utilizan el sistema fuera de las instalaciones en sus Laptop personales.
	A.11.7.2	☒ SI ☐ NO	En la organización se emplea la comunicación remota y el uso de VPN para el uso del sistema
A.12.1: Requisitos de seguridad de los sistemas de información	A.12.1.1	☒ SI ☐ NO	La seguridad se contempla en el desarrollo o modificación de nuevos proyectos informáticos pero no a un nivel formal
A.12.2: Procesamiento correcto en las aplicaciones	A.12.2.1	☒ SI ☐ NO	Control de validación de datos de entrada de forma informal
	A.12.2.2	☐ SI ☒ NO	Contemplado dentro del control 10.6.1
	A.12.2.3	☒ SI ☐ NO	Falta de personalización de firmas personales en los mensajes de correo electrónico o en el chat de mensajería
	A.12.2.4	☒ SI ☐ NO	Los resultados se revisan en los reportes. Pero falta un procedimiento formal que verifique la integridad de los resultados.
A.12.3: Controles criptográficos	A.12.3.1	☒ SI ☐ NO	La información sensible no tiene mayor protección que la que le da su usuario propietario.

	A.12.3.2	☒ SI ☐ NO	El personal no está socializado con la importancia del uso de claves robustas
A.12.4: Seguridad de los archivos del sistema	A.12.4.1	☒ SI ☐ NO	Falta de procedimientos formalizados para la instalación de aplicaciones software sobre un sistema operativo en producción sobre todo a nivel de equipos sensibles como los servidores
	A.12.4.2	☒ SI ☐ NO	No se dispone de protección para los datos de prueba. Los datos de prueba revelan procesos estratégicos de negocio.
	A.12.4.3	☒ SI ☐ NO	El acceso al código fuente es para los administradores pero conviene que se apliquen medidas de seguridad más estrictas
A.12.5: Seguridad en los procesos de desarrollo y soporte	A.12.5.1	☒ SI ☐ NO	Actualmente control de cambios a nivel informal y sin documentación y procedimientos
	A.12.5.2	☒ SI ☐ NO	Falta de procedimientos preproducción para probar el funcionamiento de nuevas implementaciones de sistema operativo para equipos críticos de negocio.
	A.12.5.3	☒ SI ☐ NO	Políticas necesarias sobre todo en equipos servidores debido a que son las centrales principales de procesamiento de datos.
	A.12.5.4	☐ SI ☒ NO	Contemplado dentro del control 12.5.1
	A.12.5.5	☐ SI ☒ NO	El software se desarrolla por

			terceras partes pero dentro de la organización mediante un contrato.
A.12.6: Gestión de vulnerabilidad técnica	A.12.6.1	☒ SI ☐ NO	Continuar con las medidas investigativas para informarse sobre nuevas vulnerabilidades que pueden presentar las aplicaciones que se utilizan en la organización, pero esta vez periódicamente
A.13.1: Reportar eventos y	A.13.1.1	☒ SI ☐ NO	Los reportes de eventos de seguridad es rápido pero debería ser documentado como aprendizaje para futuros incidentes
	A.13.1.2	☒ SI ☐ NO	Fortalecer el Plan de Seguridad de riesgos mediante retroalimentación
A.13.2: Gestión de los incidentes y mejoras de seguridad de la información	A.13.2.1	☒ SI ☐ NO	El Plan de Gestión de riesgos requiere de la colaboración y apoyo del personal
	A.13.2.2	☒ SI ☐ NO	Cuantificar el daño para saber si la inversión vale la pena
	A.13.2.3	☐ SI ☒ NO	La organización no se enfoca en este tipo de incidencia debido a la naturaleza de la organización
A.14.1:Aspectos de seguridad de la información de la gestión de continuidad del negocio	A.14.1.1	☐ SI ☒ NO	No aplica en el presente trabajo de graduación
	A.14.1.2	☐ SI ☒ NO	No aplica en el presente trabajo de graduación
	A.14.1.3	☐ SI ☒ NO	No aplica en el presente trabajo de graduación
	A.14.1.4	☐ SI ☒ NO	No aplica en el presente trabajo de graduación
	A.14.1.5	☐ SI ☒ NO	No aplica en el presente trabajo

			de graduación
A.15.1: Cumplimiento de requisitos legales	A.15.1.1	☒ SI ☐ NO	Asociación con leyes como: Seguridad Laboral y ocupacional, Derecho tributario, Ley de Compañías, Derechos y obligaciones del empleado y del empleador,
	A.15.1.2	☒ SI ☐ NO	Falta de regulación de temas de derechos de propiedad intelectual que puede traer consigo problemas legales
	A.15.1.3	☒ SI ☐ NO	Protección de documentos de carácter legal
	A.15.1.4	☒ SI ☐ NO	La información personal, tanto de los empleados como de los clientes es privada y de uso interno de la organización.
	A.15.1.5	☒ SI ☐ NO	Falta de socialización sobre temas de seguridad al personal
	A.15.1.6	☐ SI ☒ NO	La organización únicamente mantiene información del personal y de clientes que son de interés público y legal, no se dispone de información confidencial.
A.15.2: Cumplimiento de las políticas y normas de seguridad y el cumplimiento técnico	A.15.2.1	☒ SI ☐ NO	Una vez implementado el sistema, para mantener la eficacia del sistema es recomendable este control
	A.15.2.2	☒ SI ☐ NO	Cada cambio que se genere en la empresa con fines de expansión debe contemplarse para el Plan de Seguridad
A.15.3: Consideraciones de auditoria de los sistemas de información	A.15.3.1	☐SI ☒ NO	La importancia de las auditorías externas para obtener resultados del estado del SGSI desde un punto de vista arbitrario

	A.15.3.2.	☐ SI ☒ NO	Las herramientas de auditoria las posee el organismo externo, fuera de los alcances de la organización.

Tabla 18: Aplicabilidad de controles ISO 27001:2005
(A. G. Gomez)

5.3. Valoración costo beneficio del sistema

La valoración costo-beneficio es un método de estimación de la implementación de un SGSI con relación a los riesgos a los que está expuesta la empresa en términos de Seguridad de la Información. Esta valoración muestra la implementación desde un punto de vista económico y no solo técnico, de esta manera se puede validar que el proyecto es viable o no. A continuación en el siguiente cuadro se analizarán los recursos que se utilizaran para la implementación según las salvaguardas seleccionadas al principio de este capítulo frente al ahorro que se generará con la respuesta reactiva de la organización ante un riesgo inminente.

COSTOS/BENEFICIOS	**AÑO 1**	**AÑO 2**	**AÑO 3**
Adquisición de hardware y software	Reloj biométrico: 300 División Centro de Computo con Gypsum: 2400 Extractor de aire: 300 Adquisidor cámaras de vigilancia:3000 6100,00	0	0
Gasto Mantenimiento de hardware y software anteriores	Candado para Pc escritorio (10 PC's): 100 Soporte móvil para PC (12): 156	0	0

	Licencias Office(3): 2673 Licencias de Sistema Operativo 0(11): 1947		
	4874,00		
Gastos de comunicaciones	Cableado: 2500	0	0
	2500,00		
Gastos de instalación	Costo por obra cableado: 1200 Costo por instalación Gypsum: 800 Costo por instalación ducto de ventilación: 200	0	0
	2200,00	0	0
Gastos del mantenimiento del sistema	Soplador/año: 34 Spray de limpieza para equipos de cómputo/:16	Soplador/año: 34 Spray de limpieza para equipos de cómputo/:16	Soplador/año: 34 Spray de limpieza para equipos de cómputo/:16
	50,00	50,00	50,00
Gastos de consultoría	Consultor/año: 500	Consultor/año: 500	Consultor/año: 500
	500,00	500,00	500,00
Gastos de formación	Contratación experto/año(x2): 800	Contratación experto/año(x2):800	Contratación experto/año(x2):800
	800,00	800,00	800,00
Costes derivados de la aprendizaje de la curva de aprendizaje	Incremento de horas trabajadas personal de sistemas: 200	Incremento de horas trabajadas personal de sistemas: 200	Incremento de horas trabajadas personal de sistemas: 200
	200,00	200,00	200,00

Ahorros de adquisición de hardware y software	Costo Demanda por mantener software ilegal: 20000 Costo de licencias: 4618	0	0
	24618,00	0	0
Ahorro en mantenimiento de hardware	Reemplazo equipos de cómputo: 1000 Reemplazo ventiladores (x2) 100 Reemplazo de discos con fallas físicas (x2) 190 Revisiones por cables de red desconectados, malogrados/año: 360 Reposición de equipos host: 15000	Reemplazo equipos de cómputo: 1000 Reemplazo ventiladores (x2) 100 Reemplazo de discos con fallas físicas (x2) 190 Revisiones por cables de red desconectados, malogrados/año: 360	Reemplazo equipos de cómputo: 1000 Reemplazo ventiladores (x2) 100 Reemplazo de discos con fallas físicas (x2) 190 Revisiones por cables de red desconectados, malogrados/año: 360
	16650,00	1600,00	1600,00
Ahorro en comunicaciones	Resmas de hoja: 300 Comunicación vía telefónica privada /año: 5200	Resmas de hoja: 300 Comunicación vía telefónica privada /año: 5200	Resmas de hoja: 300 Comunicación vía telefónica privada /año: 5200
	5500,00	5500,00	5500,00
	15360,00	15360,00	15360,00

Ahorro en Consultoría	Costo análisis de un experto para levantamiento de procesos y creación de un SGSI: 10000	0	0
	10000,00	0	300
Beneficios instalación (Mejora en la atención al cliente, mejora de imagen de la compañía)	Ing.resos/año incluido capital: 33000 Avaluó empresa: 700000	Ing.resos/año incluido capital: 33000,00 Avaluó empresa: 700000,00	Ing.resos/año incluido capital: 33000,00 Avaluó empresa: 700000,00
	733000,00	734500,00	735700,00

Tabla 16: Detalle Analisis Costo Beneficio (Nivicela)

AÑO 1

	COSTO	BENEFICIO (Valoración MADECO)
Adquisición de hardware y software	6100,00	24618,00
Mantenimiento de hardware y software anteriores	4874,00	16660,00
Gastos de comunicaciones	2500,00	5500,00
Gastos de instalación	2200,00	734500,00
Gastos de aprendizaje	200,00	734500,00
Gastos de consultoría	500,00	10000,00
Gastos de formación	800,00	734500,00
Costes derivados de la curva de aprendizaje	200,00	734500,00

Tabla 17: Resumen Año 1 C/B (Nivicela)

AÑO 2

	COSTO	BENEFICIO (Valoración MADECO)
Adquisición de hardware y software	0	24618,00

Mantenimiento de hardware y software anteriores	50	1600,00
Gastos de comunicaciones	0	5500,00
Gastos de instalación	0	735700,00
Gastos de consultoría	0	0
Gastos de aprendizaje	200,00	735700,00
Gastos de formación	800,00	735700,00
Costes derivados de la curva de aprendizaje	200,00	735700,00

Tabla 18: Resumen Año 2 C/B (Nivicela)

AÑO 3

	COSTO	BENEFICIO (Valoración MADECO)
Adquisición de hardware y software	0	24618,00
Mantenimiento de hardware y software anteriores	50	1600,00
Gastos de comunicaciones	0	5500,00
Gastos de instalación	0	733000,00
Gastos de consultoría	0	0
Gastos de aprendizaje	200,00	733000,00
Gastos de formación	800,00	733000,00
Costes derivados de la curva de aprendizaje	200,00	733000,00

Tabla 19: Resumen Año 3 C/B (Nivicela)

A través de los cuadros analizados se puede contemplar que los beneficios de la implementación de los controles son mucho más beneficiosos que la exposición de las amenazas materializadas.

El proyecto es viable. Los costos utilizados son un referente a los valores que actualmente se encuentran en el mercado.

CAPITULO 6: POLÍTICAS DE SEGURIDAD

6.1. Política de seguridad de la información

Las siguientes políticas de seguridad han sido creadas a medida de la empresa, después de analizar activos, amenazas, vulnerabilidades y posibles riesgos a los que se encuentra expuesta la organización. La debida documentación se ha efectuado bajo la revisión constante y aprobación de la alta dirección, así mismo con la aprobación de los propietarios de cada proceso levantado durante la primera etapa. Estos documentos se pueden apreciar dentro de los Anexos 1 y 2 presentados al final del capítulo 6.

6.2. Organización de la seguridad de la información

Toda organización debe disponer de un conjunto de personas que velen por el cumplimiento de las políticas y normas de la Seguridad de la Información. Mismo que deben mantener en mejora continua de acuerdo a lo que exige la ISO 27001, en este caso deberán retroalimentar sus políticas con apoyo del personal propietario de los procesos, además de guiarse por las posibles actualizaciones de la Metodología MAGERIT. Es por eso que para garantizar que todas las actividades de mejora continua se lleven a cabo se sugiere la siguiente conformación:

6.2.1. Organización interna

Siguiendo la estructura de la Tabla 7: Segmentación de la estructura organizativa propuesta se sugiere:

Roles	**Asignación**
Comité de Dirección	Arq. Mauricio Heredia
	Tania Heredia
Comité de Seguimiento	Ing. Marcos Orellana

	Sr. Alfonso Heredia
	Ing. Mercedes Carrión
Equipo de proyecto	Ing. Katty Cabrera Ing. Marcos Orellana
	Fernanda Nivicela
Promotor	Fernanda Nivicela
Director de proyecto	Ing. Marcos Orellana
	Ing. Katty Cabrera
Enlace Operacional	Tania Heredia

Tabla 20: Segmentación estructura Organizativa
MADECO (Nivicela)

6.2.2. Organización de partes externas

Las brechas de seguridad provocadas por el acceso de terceros a instancias de la organización. En este puntual caso haciendo referencia a la contratación de una empresa externa que proporciona los servicios de Tecnología de Información.

CONTROL:	Organización De La Seguridad De Información
FECHA DE EMISION:	28/02/2014
VERSION DOCUMENTO:	v 1.0

Política	**Procedimiento**	**Riesgo**	**Actividades**
Sobre el control de accesos de personas u	Identificación de los riesgos relacionados a partes externas	Divulgación de información confidencial	1.-Renovacion o elaboración de contratos con terceras partes proveedoras de servicios. 2.-Realizar una revisión anual del

entidades externas			cumplimiento de términos del contrato.
	Tratamiento de seguridad con entidades externas		1.-Elaborar un contrato de acuerdo común de entrega de servicio, controlando los siguientes puntos: SLA: Compromiso de disponibilidad de servicio proporcionado NDA: Compromisos de confidencialidad de la información manipulada Términos y condiciones del contratista y del contratante. Penalizaciones o cierre del contrato por incumplimiento de responsabilidades.

6.3. Gestión de activos

Los controles de la norma especifican que se debe llevar un inventario de todos los activos indispensables para la organización, motivo que impulsó a realizar una identificación de los activos de información de acuerdo a los procesos de negocio, mismos que fueron calificados por sus propietarios para conocer el valor del activo para la empresa.

6.3.1. **Responsabilidad por los activos**

En cuanto al **inventario de activos,** deben estar actualizados frente a los cambios cada cierto periodo puesto que la protección real depende de objetos reales que requieren de protección. Para los encargados del SGSI se sugiere seguir el siguiente modelo de inventario:

CONTROL:	INVENTARIOS
FECHA DE EMISION:	dd/mm/aaaa
VERSION DOCUMENTO:	

Ubicación	**Proceso**	**Tipo**	**Activo**	**IDENTIFICADOR**

Elaborado por:	
Revisado y aprobado por:	
Numero de Paginas:	

El control del mismo puede ser llevado a cabo al momento de nuevas asignaciones o reasignaciones de activos. Por otro lado también se pueden valer de herramientas como Genos Open Source, es un software libre que proporciona al adminsitrador de la red un inventario de información general y algunos detalles de aplicaciones, sistemas operativos y características técnicas de los equipos.

Para la **propiedad de los activos** se utilizó el siguiente formato. Que responsabiliza a los empleados de cada activo según el proceso al que pertenezcan. Los responsables de cada activo asignaran el valor de cada activo dependiendo de las consecuencias que puedan provocar la pérdida de sus dimensiones de interés. *Ver Anexo 3*

CONTROL:	Propiedad De Los Activos
FECHA DE EMISION:	dd/mm/aaaa
VERSION DOCUMENTO:	

Rol	**Responsable**	**Tipo**	**Activo**

Elaborado por:	
Revisado y aprobado por:	
Numero de Paginas:	

Se debe velar además por el buen uso y mantenimiento de los activos de información, para lo mismo se debe llevar un control sobre la **utilización aceptable de los activos**. Se sugiere que como documentación y para el control se maneje la siguiente plantilla:

CONTROL:	Utilización De Activos
FECHA DE EMISION:	dd/mm/aaaa
VERSION DOCUMENTO:	

Área	**Actividad**	**Activo**	**Responsable**	**Fecha de Control**

Elaborado por:	
Revisado y aprobado por:	
Numero de páginas:	

Las actividades que se deben coordinar pueden ser:

6.3.2. Clasificación de la información

Se ha realizado la tasación de activos de acuerdo a la exigencia de la norma ISO 27001:2005, para lo mismo se ha utilizado la valoración Delphi que sugiere la Metodología MAGERIT (Públicas, MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol III).

CONTROL:	Directrices de Calificación
FECHA DE EMISION:	dd/mm/aaaa
VERSION DOCUMENTO:	

Activo de Información	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Total**

6.4. Seguridad de los recursos humanos

Se tiene completa conciencia de que los recursos humanos internos y externos forman parte importante de la empresa, puesto que ellos son los que están en contacto directo con los activos, por tanto hay que educarlos de manera que todos estén familiarizados con las políticas de Seguridad de la Información y su papel dentro del proceso de protección y buen empleo de los mismos.

CONTROL:	Seguridad De Los Recursos Humanos
FECHA DE MODIFICACION:	04/03/2014
VERSION DEL DOCUMENTO	V 1.0

6.4.1. **Antes del empleo**

Política	**Procedimiento**	**Riesgo**	**Actividades**
Reclutamiento	Roles y responsabilidades	Negligencia Actividades incumplidas Retraso en el cumplimiento de actividades del empleado	Definir perfiles de contratación de acuerdo al puesto que se oferte.
	Selección		1. Verificar que los documentos del curriculum encuentren actualizados y en orden 2. Verificar que se cumpla con el perfil requerido mediante

		Proceso entorpecidos por falta de cumplimiento	una entrevista
	Términos y condiciones del empleo		1. Firmar un acuerdo de confidencialidad con la empresa 2. Definir las sanciones en caso de incumplimiento de las políticas de la empresa

6.4.2. Durante el empleo

Política	**Procedimiento**	**Riesgo**	**Actividades**
Obligaciones y responsabilidades de los empleados	Responsabilidades de la dirección	No se cumplan las políticas que salvaguarden la información	Realizar una inducción al personal sobre las políticas de utilización de recursos, claves de acceso y buen uso de los activos de información.
	Toma de conciencia, educación y formación en la seguridad de la información		Socializar las políticas de seguridad de información con todo el personal sobre todo si ha habido alguna actualización de las mismas

	Proceso disciplinario		Aplicar sanciones disciplinarias en caso de incumplimiento de las políticas de la empresa

6.4.3. Terminación o cambio de empleo

Política	**Procedimiento**	**Riesgo**	**Actividades**
Terminación del contrato o dimisión del empleo	Responsabilidades de la terminación	Problemas legales con el Ministerio de Relaciones Laborales	1. "Elaborar un Acta de Finiquito, en la que debe constar que dan por terminada la relación laboral, el último sueldo percibido por el trabajador, un desglose de los valores que se cancela al trabajador (% por décimos, vacaciones, horas extras y suplementarias, fondos de reserva)." (Ecuatoriana)
	Devolución de los activos	Puesto vacío de trabajo	1. Al finiquitar el contrato el personal deberá elaborar un acta entrega de activos que le fueron asignados durante su periodo de trabajo y entregar al encargado de recursos humanos. 2. El responsable de recursos humanos se encargara de

			revisar el acta y verificar su veracidad 3. Si la entrega ha sido satisfactoria se enviara el "Acta de finiquito" al Ministerio de Relaciones Laborales
	Retiro de los derechos de acceso		Se deberá comunicar a los administradores del TI la salida del personal para que estos puedan proceder a retirar los permisos de acceso asignados.

6.5. Seguridad física y ambiental

Uno de los activos principales de la empresa son las instalaciones, debido a que sobre estos establecimientos se desarrollan las actividades comerciales y administrativas de la organización. Es por esta razón que dentro de los controles ISO 27001:2005 se especifica el objetivo de control "prevención de accesos físicos no autorizados, daños e interrupciones a las instalaciones y a la información de la organización." (A. G. Gomez)

6.5.1. Áreas seguras

Política	**Procedimiento**	**Riesgo**	**Actividades**
Seguridad de las instalaciones	Perímetro de seguridad física	Extracción de equipos de procesamiento de	1. Colocar un reloj de acceso biométrico al centro de cómputo para que únicamente el personal de sistemas

		información Pérdida económica Daños materiales a la organización	pueda Ing.resar 2. Instalación de alarmas en los puntos de acceso a los establecimientos 3. Colocar cámaras de vigilancia para monitoreo de las áreas críticas como cajas, Centro de Procesamiento de Datos, entradas y salidas de las instalaciones.
	Seguridad de oficinas, habitaciones e instalaciones	Incendio Explosión	Asegurar los accesos a las cajas de cobranzas mediante puertas aseguradas en caso de que el empleado no se encontrara dentro de la estación de trabajo.
	Protección contra amenazas externas y ambientales	Fallas por impedimento de manipulación de equipos Fallas de unidades de trabajo	1. En las todas las edificaciones se debe disponer de extintores funcionales (Valdés) 2. Creación de un plan de evacuación de emergencia.
	Trabajo en áreas seguras	Sobrecalentamiento de	1. Señalizar los accesos a áreas restrIng.idas 2. Poner señales informativas de precaución según sea el caso.

		equipos Deterioro de ciertos materiales de los equipos que provocan fallas en los mismos Accesos no autorizados	3. Instalación de extractores de aire en [L]1, [L]2, [L]3 por la salud del personal.
	Áreas de acceso al público, entrega y carga		1. Adecuación de Centro de Procesamiento de Datos: a. Ducto de ventilación. b. Aislamiento de habitación con pared falsa en vez de vidrio. c. Instalación de Splitter en el Centro de Procesamiento de Datos para seguridad de los equipos [HW][host]1, [HW][host]2, [HW][host]3 2. Instalación de un reloj de control de acceso biométrico a la habitación.

6.5.2. Seguridad de los equipos

Política	**Procedimiento**	**Riesgo**	**Actividades**
Seguridad de los equipos	Ubicación y protección del	Robo del equipo y perdida de información	1. Los CPU deben colocarse sobre una base plataforma sobre el piso, fuera de la vista al público. 2. Los dispositivos periféricos incluyendo el monitor

	equipo		deben estar asegurados con candados o amarras al CPU
	Servicio de apoyo	Detención de los servicios de impresión y procesamiento de información	1. Realizar pruebas de funcionamiento cada 2 meses para verificar que en caso de corte de energía el UPS funcione normalmente. 2. Realizar simulacros cada 6 meses simulando corte de energía para probar el funcionamiento del generador. 3. Socializar el **plan de acción en caso de corte de energía.**
	Seguridad del cableado	Perdida de comunicación interna o con otras sucursales Pérdida de calidad de conexión entre terminales	1. Re cablear las instalaciones considerando la norma EIA/TIA 568A para cableado estructurado 2. Colocación de escalerillas para protección de cableado estructurado 3. Uso de canaletas para protección de conexiones hacia las estaciones de trabajo
	Mantenimiento de equipos	Sobrecalentamiento de los equipos	1. Limpieza interna de circuitos de equipos con un spray limpiador sin agua para telecomunicaciones cada 3 meses

	Seguridad en la reutilización o eliminación de equipos	Fallas de unidades de trabajo Uso limitado de características de las aplicaciones y problemas legales	1. Licenciar Sistemas Operativos o instalar sistemas operativos de código abierto 2. Licenciar Aplicaciones de ofimática e instalar las licencias que ya se dispone o reemplazar por herramientas ofimática de código abierto 3. Desinstalar y eliminar registros de software que requiere de licenciamiento y no se utiliza.

6.6. Gestión de comunicaciones y operaciones

Con este conjunto de controles se pretende asegurar que los recursos de procesamiento de información se utilicen apropiadamente y para los fines a los que están destinados, velando por la seguridad de la información. Al hablar de recursos de procesamiento de información se hace referencia a todos los tipos de activos reconocidos por la organización que se vinculan con los procesos críticos de negocio, su manipulación y control.

6.6.1. Procedimientos y responsabilidades de operación

Política	Procedimiento	Riesgo	Actividades
Operación y tratamiento de recursos de información	Documentación de Proceso operativos	Negligencia Problemas con los clientes	1. Elaborar un conjunto de indicadores de labores para cada perfil de trabajo e indicar como llegar a cumplirlos de mejor manera. Para esto se requerirá que los jefes de cada proceso determinen cada uno de estos. 2. Implementación de un buzón de comentarios y sugerencias a nivel físico y virtual para verificar la calidad del servicio que se está ofreciendo
	Gestión de cambio	Inconsistencias de datos del sistema Funcionamiento parcial de aplicación Perdida de seguridad	1. Documentar solicitudes de cambio: fecha, solicitante, motivos, área que en la que se desea realizar el cambio, estado del cambio (solicitado, análisis, aprobado, realizado), encargado de realizar el cambio, fecha de entrega 2. Documentar vialidad del cambio 3. Establecer y documentar criterios de aceptación de cambios. 4. Comunicar si el cambio se va a realizar 5. Documentar pruebas del cambio aplicado preproducción

		Fraude Conflictos internos por inconsistencia de datos Robo de Información	6. Seguimiento durante 1 mes del cambio en entorno de producción
	Segregación de tareas		1. Aislar los cargos de compras, ventas, gerencia, dirección y contabilidad entre sí. Cada uno debe realizar sus actividades.
	Separación de los recursos para el desarrollo, prueba/ensayo y operación		1. Destinar dos equipos para pruebas preproducción 2. Instalar todas las aplicaciones que utilizan los usuarios y que requieran de configuración del personal de sistemas 3. Recopilar resultados de las pruebas 4. Corrección de errores si existieran 5. Puesta en producción del sistema con los cambios realizados

6.6.2. Gestión de entrega de servicio de tercera parte

Debido a que la empresa contrata servicios externos para la administración de Tecnología de Información, se debe procurar la formalización del mismo para aspectos referentes a términos legales, de confidencialidad y de entrega de servicio.

Política	Procedimiento	Riesgo	Actividades
Entrega de Servicios de terceras partes	Entrega del servicio	Retardo en el cumplimento de roles y tareas Negligencia	1. Elaboración de un contrato con cada proveedor de servicio en donde se plasmen aspectos de confidencialidad, disponibilidad, responsabilidades y obligaciones del contratista y del contratante, sanciones por incumplimiento de ambas partes y cláusulas de cierre del contrato. 2. Renovación del contrato cuando las dos partes consideren pertinente
	Seguimiento y revisión de los servicios de tercera parte		1. Anualmente realizar auditorías internas a cargo de la Gerencia y de un profesional de TI para validar el cumplimiento de actividades del proceso. 2. Solicitar pruebas de cumplimiento, registros, bitácoras de asistencia y de cumplimiento de cronograma de mantenimiento anual.

6.6.3. Planificación y aceptación del sistema

Es conveniente que no únicamente se lleven a cabo procedimientos informales para la gestión de cambios o nuevas implementaciones de software. Se incrementa la confiabilidad en el desarrollo del proyecto y se minimiza la incertidumbre y fallas en los sistemas.

Política	Procedimiento	Riesgo	Actividades
Planificación y aceptación del sistema	Gestión de capacidad	Funcionamiento no acorde a las necesidades del entorno que desarrollan	1. Uso y aplicación de herramientas como PMBOOK para planificación de proyectos que cubran: Alcance, Cronograma, Recursos, Riesgos, Comunicación, Calidad e Inversión 2. Uso de las normas internacionales ISOTEC 11801 y EIA/TIA 586 CSA de cableado estructurado

6.6.4. Protección contra código malicioso y movible

Se notó que la organización no protege completamente sus equipos contra estas amenazas y los usuarios no están conscientes de los riesgos de seguridad que se pueden presentar.

Política	Procedimiento	Riesgo	Actividades
Protección de integridad de software y de la información	Control contra código malicioso	Spam	1. Búsqueda de un antivirus que cumpla con las necesidades del negocio (kaspersky, Microsoft essentials, Windows defender) 2. Instalar y configurar el antivirus de manera que se ejecuten actualizaciones y análisis programados 3. Controlar mensualmente las estadísticas de código malicioso eliminado, objetos en cuarentena, errores de actualización o

			de análisis.
	Control contra código movible	Virus, troyanos, rootkits	1. Socializar a los usuarios los riesgos de abrir archivos desconocidos, lectura de dispositivos externos sin previo análisis de virus, ejecución de aplicaciones desconocidas y navegación segura. 2. Bloquear permisos de ejecución de software para usuarios operadores 3. Gestiónar proxy de internet para navegación segura y filtrada de contenido.

6.6.5. Copia de seguridad

No existe un procedimiento de copias de respaldo para los archivos, base de datos, configuraciónes de usuarios operadores y administradores que asegure estos activos en caso de pérdida, robo o alteración de información.

Política	**Procedimiento**	**Riesgo**	**Actividades**
Integridad y disponibilidad de recursos e	Copia de Seguridad de la información	Perdida de disponibilidad de información	1. Analizar la posibilidad de hacer respaldos de Base de Datos en la nube 2. Analizar la adquisición de un dispositivo externo para

información			respaldos locales y de configuración 3. Analizar el tipo de respaldo requiere la información: incremental, completa, diferencial, copia o respaldo diario. 4. Realizar un cronograma de respaldos

6.6.6. Gestión de seguridad de la red

Política	**Procedimiento**	**Riesgo**	**Actividades**
Protección de la información y de infraestructura de red	Control de red	Ataques hacker , cracker	1. Análisis de componentes o software que facilite la exportación de reportes de trafico de red administrativo y publico 2. Desactivar las actualizaciones automáticas y cada mes verificar actualizaciones. 3. Actualizar únicamente módulos de seguridad y alguna actualización que convenga a la organización 4. Escaneo y gestión de puertos abiertos cada mes
	Control de Servicios de Red	Detención de los servicios	1. Elaborar un diagrama de infraestructura de TI de todas las redes segmentadas

		de red	2. Revisión semanal de logs de acceso a aplicaciones de red.

6.6.7. Manejo de medios de información

Política	Procedimiento	Riesgo	Actividades
Control de manipulación de la información	Procedimientos de manejo de la información	Alteración y/o robo de información	1. Capacitar al personal sobre almacenamiento de documentos, organización y codificación de los mismos 2. Concientización de los usuarios sobre la eliminación de información de dispositivos externos 3. Política de escritorio físico y pantalla limpios
	Seguridad de la documentación de sistemas		1. Analizar la posibilidad de instalación de un software que proteja la información por ejemplo se puede utilizar el freeware pathlock 2. Indicar a los usuarios como manipular este software

6.6.8. Intercambio de información

La empresa se relaciona con entidades externas tales como el SRI, Proveedores, Bancos, por tanto es importante considerar métodos que garanticen que el proceso se ha realizado de forma segura.

Política	**Procedimiento**	**Riesgo**	**Actividades**
Intercambio de información y software con entes externos	Políticas y procedimientos de intercambio de información	Mala publicidad	1. Capacitar a los usuarios para que no guarden contraseñas, ni datos enviados o cargados en formularios en línea, acceso a páginas seguras para trámites en línea. 2. Configurar navegadores para que se borren los cookies, contraseñas, historiales de autocompletado.
	Medios de información físicos en transito	Perdida de respaldos de información valiosa	1. Guardar los medios físicos de respaldo en cajas con las respectivas seguridades para que no se golpeen o malogren durante el envío. 2. Traslado de los medios del Centro de procesamiento de Datos a [L]3 a un armario o un espacio aislado y asegurado
	Mensaje electrónico	Robo de información	1. Capacitar al personal para que la información sensible la encripte bajo contraseña, comprima y envíe al destinatario. 2. Las claves deben contener como mínimo letras mayúsculas, minúsculas y números
	Sistemas de información del		1. Analizar las políticas de seguridad planteadas en el presente trabajo de graduación

	negocio		2. Ajustar a nuevas necesidades encontradas 3. Implementar el SGSI

6.6.9. Servicios de comercio electrónico

La empresa actualmente posee un sitio web informativo que está disponible para público en general y para clientes. Según las proyecciones a futuro para transacciones en línea se propone lo siguiente:

Política	**Procedimiento**	**Riesgo**	**Actividades**
Comercio electrónico seguro	Información disponible públicamente	Robo de información Alteración de información	1. El administrador del sitio debe usar contraseñas robustas que contengan: Mayúsculas, minúsculas, números y caracteres especiales 2. Exigir que el sitio web se desarrolle con manejo de sesiones, sesiones inactivas y notificación de inicio de sesión al administrador

6.6.10. Seguimiento

Toda actividad deberá ser registrada, en caso de que se encuentre alguna irregularidad se puede seguir la trazabilidad del proceso en caso de necesidad de investigación. Se deben registrar todo tipo de actividades y eventos

Política	**Procedimiento**	**Riesgo**	**Actividades**
Trazabilidad de acceso a la información	Registro de Auditoria	Conflictos internos Problemas legales Mala publicidad	1. Elaborar un documento de indicadores de cumplimiento de cada proceso 2. Auditar cada uno de los procesos 3. Elaborar un informe final de cumplimientos y no conformidades que deben ser corregidas
	Seguimiento de la utilización de los sistemas		1. Ajuste en el Sistema DOCS para registrar: a. Eventos de seguridad b. Actividades de los usuarios
	Protección de la información de registro	Perdida de información	1. Archivar los registros de auditoria, de actividad de servidores, red y acciones correctivas de forma lógica y/o física
	Administrador y operador de registro		1. Realizar ajustes de la aplicación DOCS para registrar actividades y parámetros de los administradores y de los usuarios operadores en caso de modificación o actualización de base de datos o del aplicativo mismo. 2. En caso de producirse un error en la ejecución o validación se

			debe recurrir a la revisión de registros 3. Revisar los registros de actualización y modificación mensual para revisar irregularidades
	Registro de fallas		1. Elaborar un formulario que dispongan los usuarios para reportar incidentes para su posterior atención 2. Elaborar formatos de registro de incidencias con información referida a: Fecha de incidencia, hora, incidente, causa, solución, ejecutado por 3. Mantener los registros actualizados
	Sincronización de relojes	Inconsistencia de información	1. Sincronizar los relojes del sistema con el reloj de los servidores centrales 2. Verificar diariamente que el reloj de los servidores principales sea correcto 3. Los registros de actividad deben registrar la hora del servidor.

6.7. Control de accesos

Mediante las políticas de acceso se pretende mitigar las brechas de seguridad producidas por abuso de privilegios de acceso y accesos no autorizados.

CONTROL:	CONTROL DE ACCESO
FECHA DE EMISION:	05/03/2014
VERSION DOCUMENTO:	v1.0

6.7.1. Requisitos del negocio para el control de accesos

El centro de Procesamiento de Información no es adecuado y es propenso a sufrir riesgos de seguridad de acceso, contaminación y mal funcionamiento mecánico.

Política	**Procedimiento**	**Riesgo**	**Actividades**
Requisitos de negocio para control de acceso	Control de acceso	Modificación de información Extracción de equipos de procesamiento de	1. Instalación de un reloj de control de acceso biométrico en la puerta 2. Aislamiento de la habitación y reemplazo de fachada de vidrio por paredes falsas

		información Destrucción de información	3. Reemplazo de la puerta corrediza por una más segura.

6.7.2. Gestión de acceso de usuarios

La formalización de las actividades durante el contrato y al finalizar el contrato del personal que tiene acceso al aplicativo comercial de la empresa debe regirse por las siguientes políticas

Política	**Procedimiento**	**Riesgo**	**Actividades**
Gestión de acceso de usuarios	Registro de usuarios	Abuso de privilegios de acceso	1. Registrar en una plantilla de Ing.reso de personal: tipo de accesos requeridos, aplicaciones a utilizar. 2. Enviar oportunamente el formulario al Departamento Sistemas para que puedan adecuar el espacio de trabajo y configurar los respectivos accesos al sistema. 3. Hacer la entrega de las herramientas y recursos tecnológicos que va a utilizar con una inducción a la seguridad de información 4. Firmar la entrega recepción del formulario de requisitos entregado en primera instancia.

	Gestión de privilegios		1. Documentar los usuarios del sistema y sus privilegios de acceso. 2. Validar que todos los accesos sean los que se han autorizado y aprobar los documentos que certifican estos accesos.
	Gestión de contraseñas de usuarios		1. Asignar contraseñas a los usuarios que se personalicen al primer inicio de sesión 2. Las contraseñas asignadas deben ser robustas y no seguir una misma tendencia (ejm: la00, ah00, aheredia1, mheredia1, etc.)

6.7.3. Responsabilidades de usuarios

Política	**Procedimiento**	**Riesgo**	**Actividades**
Responsabilidades de los usuarios	Uso de contraseñas	Robo de información Alteración de la información	1. Inducir a los usuarios operadores en la seguridad de información sobre las consideraciones de seguridad para asignación de contraseñas 2. Los aplicativos deben configurarse para exigir a los empleados el registro de claves robustas

	Equipos desatendidos		1. Cuando se vayan a alejar de sus estaciones de trabajo los usuarios deberán bloquear la sesión que se está utilizando 2. Cerrar documentos que no se estén utilizando
	Política de escritorios pantallas limpias		1. Organizar los documentos y guardarlos en el directorio documentos de usuario o en el directorio raíz. 2. El escritorio solo debe contener accesos directos a las aplicaciones que utiliza 3. Los documentos tales como cheques, letras de cambio, comprobantes de pago, facturas de proveedores y de clientes deben estar guardados en las garitas de los escritorios o en un área trasera al usuario donde solo éste pueda acceder.

6.7.4. Control de acceso a la red

La red se encuentra segmentada en LAN Administrativa para acceder a servicios de Sistema de Información y Wifi publico utilizado para servicios de internet.

Política	**Procedimiento**	**Riesgo**	**Actividades**
Acceso a la red	Utilización de servicios de red	Robo de información Alteración de la información	1. Compartir los archivos para un numero definido de usuarios o un usuario definido 2. El archivo debe configurarse con privilegios de lectura y/o escritura según sea el caso
	Autenticación de usuarios para conexiones externas	HackIng., CrackIng.	1. Configurar las aplicaciones para conexión remota con contraseñas robustas que contengan: Mayúscula, minúsculas, números y caracteres especiales. 2. Configurar el acceso a la red únicamente por puertos definidos y permisos de acceso remoto a equipos definidos.
	Identificación de equipo en redes		Definir que ip corresponden a los equipos que deben manipular el sistema de información dentro de las instalaciones y asignar privilegios de acceso únicamente al listado reconocido.
	Protección del diagnóstico remoto y de la configuración del puerto		1. Configurar el firewall para bloquear o controlar el tráfico por puertos sensibles como: FTP, ssh 2. Periódicamente deberán revisar los puertos abiertos mediante herramientas de escaneo y cerrar o bloquear el tráfico por

			puertos no autorizados
	Segregación en redes		1. Segregar la red pública Wifi de la LAN en todas las localidades de la empresa. 2. Creación de Redes Virtuales Privadas para conexión entre establecimientos
	Control de conexión en redes		1. Búsqueda de un software de control IDS (Detección de intrusiones) según necesidad de negocio) 2. Comunicación y aprobación de Gerencia 3. Instalación y configuración del software 4. Verificar reportes semanales de ataques o intentos de intrusión a la red. 5. Bloquear ataques 6. Agregar ip intrusiva a la lista negra de los servidores

6.7.5. Control de acceso al sistema operativo

Se realiza el control pero no a un nivel formal como política y obligación de los usuarios y administradores de la Tecnología de Información.

Política	Procedimiento	Riesgo	Actividades
Control de acceso a estaciones de trabajo	Procedimientos de conexión segura	Errores al ejecutar aplicaciones	1. Configurar accesos de usuario y administrador en los equipos 2. Configurar contraseñas de usuario y administrador
	Utilización de las prestaciones del sistema		1. Configurar en los equipos para que únicamente los administradores del sistema puedan instalar aplicaciones
	Sesión inactiva		1. Configurar el bloqueo de pantalla para desbloqueo con contraseña por cada 5 minutos de inactividad
	Limitación del tiempo de conexión	Uso inadecuado de activos	1. Configuración de proxy de internet para navegación solo a sitios autorizados en horarios de trabajo. 2. Elaborar una lista de sitios a los que la empresa permite acceder durante horarios de trabajo

6.7.6. Control de acceso a las aplicaciones e información

Política	Procedimiento	Riesgo	Actividades
Control de acceso	Restricción de	Robo de información	1. Eliminar y ocultar accesos directos a aplicaciones antivirus y

a las aplicaciones	acceso a la información	Alteración de la información	de acceso remoto 2. Análisis y selección de una herramienta de encriptación de archivos 3. Instalación de herramienta de encriptación en los equipos host del Centro de –Procesamiento de Información

6.7.7. Computación móvil y trabajo a distancia

Política	**Procedimiento**	**Riesgo**	**Actividades**
Control de trabajo remoto	Computación móvil y comunicaciones	Ataques hacker, cracker Robo de información	1. Elaborar un checklist de revisión de controles para equipos portátiles. 2. De requerirse configuración de aplicaciones corporativas en Smartphone, verificar que el dispositivo tiene antivirus y esta actualizado.
	Trabajo a distancia	Alteración de información Eliminación de información	1. Configurar el firewall para que un equipo externo pueda conectarse remotamente a través de un conjunto de puertos controlados 2. Agregar la ip del equipo que requiere de conexión a la lista de ips permitidas como conexión entrante

			3. Configurar contraseñas robustas con números, letras y caracteres especiales en las aplicaciones con las que se establecerá la conexión.

6.8. Adquisición, desarrollo y mantenimiento de información

Se ha visto que esta área se encuentra bien desarrollada pero no a un nivel formal sino a que se encuentran en un nivel ad-hoc en donde los procesos se llevan a cabo de forma desordenada.

CONTROL:	Adquisición, Desarrollo Y Mantenimiento De Información
FECHA DE EMISION:	05/03/2014
VERSION DOCUMENTO:	V1.0

6.8.1. Requisito de seguridad de los sistemas de información

Política	**Procedimiento**	**Riesgo**	**Actividades**
Seguridad de los sistemas de	Análisis y especificación de	Perdida de continuidad de servicio	1. Evaluar un conjunto de métricas de calidad de la norma IEEE, CMM (Modelo de Madurez), QIP (Paradigma de

información	requisitos de seguridad	Retraso en el procesamiento de información	mejoramiento de calidad) 2. Documentar resultados de medición 3. Comunicar a la Alta Dirección 4. Realizar cambios necesarios 5. Documentar cambios

6.8.2. Procesamiento correcto en las aplicaciones

Política	**Procedimiento**	**Riesgo**	**Actividades**
Uso correcto de las aplicaciones	Validación de datos de entrada	Inconsistencia de datos del sistema	1. Validar: cedula, RUC, Pasaporte, campos numéricos, dirección de correo electrónico, stock, usuarios, contraseñas, descuentos, etc., a nivel de aplicación.
	Integridad del mensaje	Conflictos legales por no recepción de mensajes Retraso en el procesamiento	1. Análisis de adquisición de firma electrónica 2. Comunicación y aprobación de Gerencia 3. Implementación de firma electrónica en el servidor de correo electrónico 4. Crear firmas personales para adjuntar al pie de los correos electrónicos

		de información	5. Personalizar el tipo de letra para chat SPARK
	Validación de los datos de salida		1. Analizar reportes mensualmente: Cartera proveedores, Cartera clientes, balances, cuadres de caja. Kardex

6.8.3. Controles criptográficos

Política	Procedimiento	Riesgo	Actividades
Protección de la integridad y confidencialidad de la información con medios criptográficos	Política sobre la utilización de medios criptográficos	Acceso a información confidencial	1. Análisis de software destinado a encriptación de archivos sensibles 2. Comunicación y aprobación de la Gerencia 3. Implementación de software de encriptación 4. Capacitación al usuario sobre el uso de la herramienta
	Gestión de claves	Penetración de sistemas	1. Capacitar a los usuarios sobre el uso de contraseñas robustas que contengan letras mayúsculas, minúsculas, números y caracteres especiales

6.8.4. Seguridad de los archivos del sistema

Política	Procedimiento	Riesgo	Actividades
Seguridad de los archivos del sistema	Control de software operativo	Perdida de documentos importantes Acceso no autorizado a	1. Analizar el software requerido, considerar: soporte, casos de éxito, versiones, manuales, compatibilidad, necesidades del negocio. 2. Leer manuales e informarse sobre las experiencias al liberar la

		información confidencial	aplicación. 3. Comunicar y solicitar aprobación a Gerencia 4. Instalar la aplicación 5. Ejecutar plan de pruebas
	Protección de los datos de prueba del sistema		1. Asignar una contraseña de acceso robusta a la base de datos de prueba. 2. Encriptar SQL de datos de prueba
	Control de acceso al código fuente del programa		1. Asignar una clave robusta al equipo que dispone del código fuente del Sistema de Información 2. Almacenar el directorio del código fuente en un lugar seguro del directorio raíz 3. Encriptar el código fuente

6.8.5. Seguridad de los procesos de desarrollo y soporte

Política	**Procedimiento**	**Riesgo**	**Actividades**
Seguridad del software y de la	Procedimientos de control de cambios	Interrupción de otros servicios instalados	1. Documentar solicitudes de cambio: fecha, solicitante, motivos, área que en la que se desea realizar el cambio, estado

información de la aplicación		Fallos del sistema en producción	del cambio (solicitado, análisis, aprobado, realizado), encargado de realizar el cambio, fecha de entrega 2. Documentar vialidad del cambio 3. Establecer y documentar criterios de aceptación de cambios. 4. Comunicar si el cambio se va a realizar 5. Documentar pruebas del cambio aplicado preproducción
	Revisión técnica de aplicaciones después de los cambios de sistema operativo		1. Antes de una actualización o formateo de Sistema Operativo verificar la compatibilidad de las aplicaciones que utiliza el usuario en el nuevo sistema operativo que deseamos utilizar 2. Instalación del Sistema Operativo 3. Instalación y configuración de aplicaciones 4. Seguimiento durante 1 mes del cambio en entorno de producción
	Restricciones en los cambios a paquetes software		1. Ejecutar Plan de Pruebas *Ver Anexo 7*

6.8.6. Gestión de vulnerabilidad técnica

El departamento se preocupa por la investigación en avances de tecnología, nuevas aplicaciones, pero les falta formalización de estos procedimientos. A continuación la implementación como política

Política	**Procedimiento**	**Riesgo**	**Actividades**
Reducción de riesgo de vulnerabilidad técnica	Control de vulnerabilidades técnicas	HackIng. Brechas de seguridad no cubiertas	1. Investigar sobre nuevas amenazas, vulnerabilidades de aplicaciones en producción de la empresa. 2. Investigar cómo aplicar seguridades contra la vulnerabilidad encontrada. 3. Verificar casos de éxito con la aplicación del cambio de seguridad 4. Aplicar las instrucciones de seguridad 5. Registrar la aplicación del cambio de seguridad

6.9. Gestión de incidente de seguridad de información

Es conveniente que todos los eventos vinculados con la seguridad de los sistemas sean registrados de tal modo que pueda ser corregido oportunamente y de esta manera también creamos una base de conocimientos para solucionar problemas posteriores.

CONTROL:	Gestión De Incidente De Seguridad De Información
FECHA DE EMISION:	05/03/2014
VERSION DOCUMENTO:	v1.0

6.9.1. Reportar los eventos y debilidades de la información

Política	**Procedimiento**	**Riesgo**	**Actividades**
Reporte de eventos y debilidades del sistema	Reporte de eventos de seguridad de información	Pérdida de control de estados de servicio Caída de servicios tecnológicos importantes	1. En caso de producirse errores de actualización, conexión, errores en pantalla notificar inmediatamente mediante teléfono, correo o chat a los administradores del sistema para su revisión oportuna. 2. Documentar donde se produjo el incidente, cuál fue el incidente, causas y solución. (Base de conocimientos)
	Reporte de debilidades de información		1. Seleccionar y evaluar la posibilidad de implementación de un software de gestión de incidentes (IDS) 2. Implementar IDS 3. Monitoreo diario de los reportes de incidentes notificados o

			encontrados por la herramienta o mediante formularios físicos

6.9.2. Gestión de los incidentes y mejoras de la seguridad de la información

Política	**Procedimiento**	**Riesgo**	**Actividades**
Control de incidentes y mejoras de la seguridad de la información	Responsabilidades y procedimientos	Caída de servicios tecnológicos importantes	1. Llenar los formularios o tickets de solicitud de asistencia 2. Entregar al jefe de proceso 3. El jefe de proceso aprueba la asistencia y envía al departamento de TI 4. Se establece una jerarquía de soporte según la criticidad de la solicitud 5. Asistir remotamente, físicamente o brindar instrucciones para solucionar el problema
	Aprendizaje de los incidentes de seguridad de la información		1. Evaluar opciones de resolución para los incidentes reportados 2. En caso de que el incidente requiera de inversión de la empresa, evaluar el costo de la resolución del problema 3. Comunicar y aprobar por la Gerencia la implementación de la solución o aceptación del mismo

6.10. Cumplimientos

Debido a la naturaleza del negocio, éste se ve vinculado con varias leyes y regulaciones del Estado en cuanto al Sistema Tributario, Leyes de Trabajo, Salud Ocupacional, Superintendencia de compañías y de Telecomunicaciones. Por tanto los procesos deben orientarse a cumplir a cabalidad las obligaciones y restricciones que exigen.

CONTROL:	Cumplimientos
FECHA DE EMISION:	04/03/2014
VERSION DOCUMENTO:	V1.0

6.10.1. Cumplimiento de requisitos legales

Política	**Procedimiento**	**Riesgo**	**Actividades**
Cumplimiento de leyes y regulaciones	Identificación de la legislación aplicable	Problemas legales	1. Documentar físicamente las regulaciones actuales de la normativa Tributaria del Ecuador a. Entregar a Finanzas 2. Documentar físicamente el código Laboral actualizado del Ecuador a. Entregar a la Dirección

		Perdidas económicas	3. Documentar físicamente el código de la Ley SART (Salud Ocupacional) a. Entregar a la Dirección 4. Documentar físicamente el código de la Ley de Compañías a. Entregar a Finanzas 5. Documentar el código de la Ley de Telecomunicaciones, Tecnologías de Información y Comunicación a. Entregar al Departamento de TI 6. Documentar los códigos de la Ley Orgánica de Defensa al Consumidor a. Entregar y socializar con el personal de ventas
	Derechos de propiedad intelectual	Mala publicidad	1. Verificar reportes de inventarios de aplicaciones mediante las herramientas instaladas para monitoreo de red 2. Controlar que las aplicaciones instaladas no violen el código de Propiedad Intelectual 3. Regularizar las aplicaciones que no corresponden a las autorizadas por Gerencia y el Departamento de Sistemas 4. Eliminar las aplicaciones no autorizadas

			5. Registrar el incidente
	Protección de los registros de la organización		1. Organizar y almacenar en un archivador todos los documentos legales tales como: contratos internos con los empleados, contratos externos con proveedores, permiso de funcionamiento. 2. Adecuar fiscalmente el archivador para que únicamente tengan acceso el personal autorizado.
	Protección de los datos y de la privacidad de la información		1. Planificación de capacitación sobre seguridad de la información 2. Selección de un profesional que imparta y socialice las políticas de seguridad y el plan de Gestión de Riesgos 3. Realizar la capacitación
	Prevención del mal uso de los recursos de procesamiento de la información		1. Planificación de capacitación sobre seguridad de la información 2. Selección de un profesional que imparta y socialice las políticas de seguridad y el plan de Gestión de Riesgos 3. Realizar la capacitación

6.10.1.2. Cumplimiento de las políticas y normas de seguridad de cumplimiento técnico

Política	Procedimiento	Riesgo	Actividades
Cumplimiento de políticas y normas de seguridad	Cumplimiento con las políticas y normas de seguridad	Fracaso en la implementación del SGSI	1. Cronograma un reunión periódicamente con los jefes de proceso para evaluar los cumplimientos de las políticas de Seguridad 2. Analizar cumplimiento de los indicadores de éxito de la empresa con la alineación estratégica del SGSI 3. Proponer nuevos indicadores de éxito para la empresa y los parámetros para su cumplimiento
	Comprobación del cumplimiento técnico		1. Actualizar inventarios de activos cada vez que se asigne o incorpore un nuevo usuario 2. Actualizar el listado de procesos (creación o modificación) 3. Actualizar listado de amenazas 4. Actualizar matriz de riesgos por aparición de nuevas amenazas 5. Actualizar listado de riesgos (cada amenaza saca a flote diversas vulnerabilidades) 6. Actualizar Políticas de Seguridad 7. Actualizar Plan de Gestión de Riesgos

			8. Incorporar Planes de ContIng.encia

6.10.2. Consideraciones de auditoria de los sistemas de información

Este control se debe llevar a cabo como contratación de servicios externos dado el tamaño de la organización. La parte externa se encargara de analizar y revisar el cumplimiento de Políticas de Seguridad expuestos y aspectos no considerados dentro de las mismas de manera que se impulsa la transparencia de ejecución de los procesos y un punto de vista arbitrario a los procedimientos implementados.

Conclusiones

A pesar de considerar necesaria la implementación de un Sistema de Gestión de Seguridad de la información como pilar del Plan de Gestión de Riesgos, la falta de apoyo hacia el mejoramiento de Tecnologías de Información por considerarlo no prioritario fue uno de los principales problemas de la organización. Debido a esta particularidad se encontró un Sistema de Gestión de Seguridad de la Información en un nivel base, ad-hoc, en donde pocos son los puntos considerados, en este caso la Seguridad en el Desarrollo Software, donde se presentan procesos proactivos. Sin embargo la Seguridad de la Información contempla un horizonte más amplio.

Con el planteamiento del proyecto y con el avance del mismo se fue concientizando a la Alta Dirección de la importancia de la protección de sus activos y las ventajas de alinear sus planes estratégicos con los de Tecnología de Información para alcanzar sus metas comerciales. A lo largo del planteamiento del problema no únicamente se recibió el apoyo de la Alta Dirección, sino también el compromiso de los usuarios, que básicamente es un punto a favor del éxito para la futura implementación del SGSI.

Tal y como se plantea en la norma ISO 27001:2005, a través de la Metodología MAGERIT se pudo generar cada una de las directrices y controles propuestos con un leve ajuste al tamaño y necesidad de la organización, donde se pudo observar que los servicios que ofrece el departamento de Tecnología de Información son considerados vitales para el desempeño y función de la organización. Servicios tales como el Sistema de Procesamiento de Información Comercial, correo, voz, almacenamiento de información, internet, trabajo a distancia, compartición de archivos en red son servicios utilizados por la organización para cumplir con sus labores. Estos servicios asociados con los soportes físicos se consideran dentro de este documento para ser protegidos con la implementación de las políticas de Seguridad.

Se concluye el presente estudio con los resultados finales del análisis de activos, amenazas, vulnerabilidades plasmados en un Plan de Gestión de Riesgos alineados con las Políticas de Gestión de Seguridad de la Información, en donde cada riesgo valorado puede ser mitigado mediante controles y un conjunto de actividades en las que todos los que conforman MADECO deben colaborar. Este plan esta generado para la aplicabilidad dentro de la Organización MADECO Cía. Ltda., para que pueda controlar, mitigar o eliminar cualquier riesgo tomado en cuenta dentro del análisis, previniendo en mayor grado la obstrucción de operatividad.

Recomendaciones

En este Trabajo de Graduación se propone un modelo de Organización de la Seguridad de la Información para poder apoyar e impulsar el desarrollo del Sistema de Gestión de Seguridad de la Información, se propone tomar en cuenta este modelo para la implementación y mantenimiento del SGSI.

Como primera recomendación se hace hincapié en la implementación del Plan de Gestión de Riesgos, es una alternativa muy efectiva dado el nivel de dependencia de la organización hacia las Tecnologías de Información.

Los activos de la organización debería ser etiquetados apropiadamente utilizando los códigos generados en el *Anexo 4,* de esta manera se puede llevar un mejor control de asignaciones, informes y monitorización de desempeño de los mismos.

Se dispone de licencias legales de Software que no han sido implementadas, por lo que lógicamente la legitimidad de los aplicativos es invalida. Además se posee pocas licencias en relación a la cantidad de aplicativos instalados, por lo que se recomienda comprar las licencias de todos lo aplicativos u optar por software libre, Ubuntu es una buena opción debido a la similitud con los sistemas Windows, además de poder contar con aplicaciones que simulen entornos Windows.

Con respecto a las instalaciones en donde se desempeña el Centro de Procesamiento de Información se sugiere adecuar la habitación de tal manera que los equipos puedan rendir correctamente y no deteriorarse con el paso del tiempo. De igual manera con el resto de estaciones de trabajo o terminales desde donde se genera la información. No obstante la seguridad del entorno donde se desenvuelve la organización se encontró como parte fundamental de la organización en donde se encontró que los riesgos naturales son difíciles de mitigar por tanto se sugiere

considerar la posibilidad de transferir el riesgo a terceros, como puede ser una aseguradora.

No está por demás volver a mencionar que la Alta Dirección, así como el personal en general deberá aportar con su compromiso para una implementación exitosa del Plan. Por otro lado el Plan es tolerante a cambios o ajustes que puedan producirse a lo largo de la existencia de la empresa, de manera que el Plan de Seguridad siempre este actualizado y en mejoría.

Finalmente se recomienda tomar en consideración la implementación de un Plan de Continuidad de Negocio, que abarque todos los tópicos de: Planes de acción frente a desastres y Recuperación después de desastres.

Glosario

Activos: Son todos aquellos recursos de información que tienen valor para la empresa.

Amenazas: Situaciones o eventos causados de forma intencional, por error o naturalmente provocados que por si solos no tienen validez si no existe una vulnerabilidad que puedan explotar.

Vulnerabilidades: Brechas de seguridad causadas por la falta de control o debilidades de sistemas, aplicaciones o falta de cultura de Seguridad de la Información.

Riesgos: Es la combinación de una amenaza y una vulnerabilidad que actuando al mismo tiempo pueden causar un impacto negativo sobre un activo

Salvaguardas: Medidas que se formulan para poder controlar, evitar o mitigar un riesgo inminente.

Políticas: Conjunto de procedimientos utilizados para la protección de activos de información.

Impacto: Magnitud del daño sobre un activo que significa para la empresa. (Dinero, imagen, etc.)

CMM (Modelo de Capacidad y Madurez): Es un Modelo de Evaluacion de Calidad de Desarrollo de software.

ISOTEC 11801: Norma estándar para planificación e implementación de cableado estructurado

EIA/TIA 586 CSA: Normas estándares para cableado de redes de comunicación.

Checklist: Lista de consideraciones a tomarse en cuenta para la toma de desiciones

Confidencialidad: Propiedad de los activos que tienen un dominio de conocimiento limitado.

Integridad: Propiedad de los activos de información que no pueden ser alterados o eliminados.

Disponibilidad: Capacidad de los activos de información de estar presentes o accesibles siempre cuando se los necesite.

Segregación de funciones: Separación o aislamiento de funciones para que no sean manejadas por una misma persona.

Bibliografía

Alan Calder, Steve G. Watkins. *Information Security Risk Management for ISO27001/ISO27002*. United Kingdom: Editorial IT Governance Ltd 2007, 2007.

Areitio, Javier. *Seguridad de la Informacion*. Madrid: PARAINFO, 2008.

Arjona Torres, Miguel. *Dirección estratégica. Un enfoque práctico: principios y aplicaciones de la gestión del rendimiento*. España: Ediciones Diaz Santos, 2008. Ebrary.

Castillo, Juan Carlos Martín. *Instalaciones de telecomunicaciones*. Madrid: EDITEX, 2009.

Ecuatoriana, Asamblea Nacional. "www.recaiecuador.com." 09 06 2013. 12 02 2014. <http://www.recaiecuador.com/Biblioteca%20Ambiental%20Digital/Codificacion%20Codigo%20de%20Trabajo%20con%20el%20IESS.pdf>.

Gomez, Alexander G. *Diseño de un SGSI*. Bogotá: Alfaomega Colombiana S.A, 2007.

Gomez, Alvaro. *Enciclopedia de la Seguridad Informatica*. España: RaMa Editorial, 2011.

Heredero, Carmen de Pablos, et al. *Dirección y gestión de los sistemas de información en la empresa*. Madrid: ESIC, 2008.

Laborales, Ministerio de Relaciones. "http://www.relacioneslaborales.gob.ec/." 12 2012. 27 02 2014. <http://www.relacioneslaborales.gob.ec/wp-content/uploads/downloads/2012/12/FORMATO-ELABORACI%C3%93N-DE-REGLAMENTO.pdf>.

Nivicela, Fernanda. *Tesis Gestion de Riesgos para MADECO*. Cuenca, 2013.

Piñeiro, Esther Martínez. "La técnica Delphi como estratefia de consutla a los implicados en la evaluacion de programas." *Revista de Investigación Educativa* (2003): 463.

Públicas, Ministerio de Administraciones. *MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol I*. 20 Junio 2006.

Publicas, Ministerio de Administraciones. *MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol II*. Madrid, 20 Junio 2006.

—. *MAGERIT Versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información vol III*. 20 Junio 2006.

Security Managment Consulting International. *Security Managment Consulting International, LLC*. n.d. 15 Enero 2013. <http://smcintl.com/services-offered.html>.

Tangient LLC. *Seguridad informatica*. Diciembre 2013. <http://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM>.

Valdés, Julio Téllez. *Contratos, riesgos y seguros informáticos*. Mexico: UNAM, 1988.

Anexos

Anexo 1
Plan de Gestión de Riesgos

MADECO CIA. LTDA.

Informe Preliminar

Versión 2.0

Fecha de emisión: _ _-_ _-_ _ _ _

Fecha de revisión: _ _-_ _-_ _ _ _

Fecha de aprobación: _ _-_ _-_ _ _ _

Elaborado por:	Aprobado por:
_____	_____
Fernanda Nivicela	Arq. Mauricio Heredia

Antecedentes y Justificación

Una de las problemáticas que afectan el desarrollo y buen funcionamiento de una empresa es la falta de un sistema de gestión de riesgos. Además también existen varios factores capaces de causar serios problemas financieros o de imagen con los clientes y proveedores de la empresa, ya sea por el incumplimiento en el tiempo de entrega de un producto o servicio o por que no se esté cumpliendo con la misión que inicialmente se planteó la empresa durante su creación.

Muchos de estos pueden ser el resultado de riesgos que no han sido neutralizados con un análisis y tratamiento previo de todos los activos de información así como los operacionales (en caso de haberlos). Por lo que se propone una solución viable para la continuidad del negocio previo a un desastre, en este caso un sistema de gestión de riesgos que sea capaz de mitigar todas las vulnerabilidades propensas a convertirse en riesgos para la organización, garantizando de esta manera disponibilidad, integridad y confidencialidad de la información de la empresa, es por eso que la siguiente tesis plantea seguir el modelo de seguridad de la información de la ISO 27001 que es la única norma certificable encargada de proporcionar parámetros y lineamientos que garanticen la seguridad de los activos de la empresa

Objetivos:

General

Crear un plan de gestión de riesgos de la información basada en la norma ISO 27001:2005, acorde a los controles y directrices que propone esta norma para la empresa Madeco Cía. Ltda.

Específicos

Realizar un levantamiento de activos de información de la empresa MADECO Cía. Ltda.

Analizar y clasificar los activos de la información en una jerarquía tal que denote la importancia que juega cada uno con respecto a la misión de la empresa

Identificar y analizar todas las amenazas posibles, su grado de impacto y el nivel de ocurrencia con el que se puedan suscitar.

Identificar y analizar las vulnerabilidades que pueden ser explotadas por las amenazas y convertirse en riesgos para la empresa

Generar un plan de seguridad para cumplir con los controles (ISO 27001:2005).

Alcance y delimitación

MADECO Cía. Ltda. es una empresa dedicada a la venta de materiales de construcción, está compuesta por cuatro almacenes de los cuales se va a analizar a la matriz principal y a una de las sucursales, para llegar a determinar vulnerabilidades que nos llevarán a establecer el tratamiento de riesgos adecuado como sugiere la norma ISO 27001.

Por tanto el plan de gestión de riesgos está destinado a cubrir todas las brechas de seguridad que la empresa podría tener, describiendo como proteger cada uno de los activos de información y sus respectivos recursos utilizados (físicos y humanos) a través de los controles establecidos por la norma.

Situación Actual de la empresa

Misión

Proveer materiales de calidad, durables, a un precio y cantidades justas. Asesorar a nuestros clientes en su compra para que mediante ella contribuyan a su bienestar y tranquilidad y a su vez al desarrollo de la infraestructura y economía del Ecuador.

Visión

Ser líder y referente en proveer acabados para la construcción en la zona sur del Ecuador.

Metas

Renovar exhibiciones y mejorar procesos para la venta incluyendo catalogo web en un plazo no mayor a 1 año.

Objetivos

Reducir costos de infraestructura sub-utilizada para obtener el mayor beneficio y mejor relación costo-precio en un plazo no mayor a 3 años.

Antecedentes sobre seguridad de los sistemas de información

Se ha determinado por medio de las entrevistas que la empresa no posee un Sistema de Gestión de Seguridad de la Información, un Plan de ContIng.encia, así como también un Plan de Continuidad de Negocio, actualmente se manejan mediante el concepto acción-reacción, que consiste en corregir errores o disfuncionalidades que se suscitan.

Aspectos a considerar dentro del dominio del proyecto:

Dentro de la estructura organizativa se definen varias unidades, las cuales según el director de la unidad de Coordinación General cumplen con las siguientes labores.

Directorio: Supervisión, organización y soporte de la empresa y de los empleados

Presidencia: Revisión periódica de desenvolvimiento de la empresa, gestión y toma de decisiones.

Gerencia: Encargada de lo concerniente a términos, acuerdos legales, administrativos, y manejo de documentos de la empresa.

Unidad de Ing.eniería en Sistemas: Mantenimiento, administración, supervisión de equipos y desarrollo de software para la empresa.

Unidad de Contabilidad: 1. Implantar el sistema contable más conveniente para la empresa. 2. Establecer el procedimiento óptimo de registro de operaciones efectuadas por la empresa (manual, mecánico o electrónico). 3. Verificar la exactitud de las operaciones registradas en libros y registros auxiliares. 4. Vigilar el cabal cumplimiento de las obligaciones fiscales. 5. Elaborar, analizar e interpretar los estados financieros. 6. Proporcionar a la dirección información confiable y oportuna para la toma de decisiones en el curso diario.

Unidad de Compras: Cotizar productos, pedidos, verificación de la calidad de los productos adquiridos, emitir informes de proveedores.

Ventas: Conocer, ofrecer los productos y motivar a los clientes a comprar.

Bodega: Manejo del sistema de inventarios y del movimiento de las existencias dentro del almacén. Control de fechas de expiración de artículos.

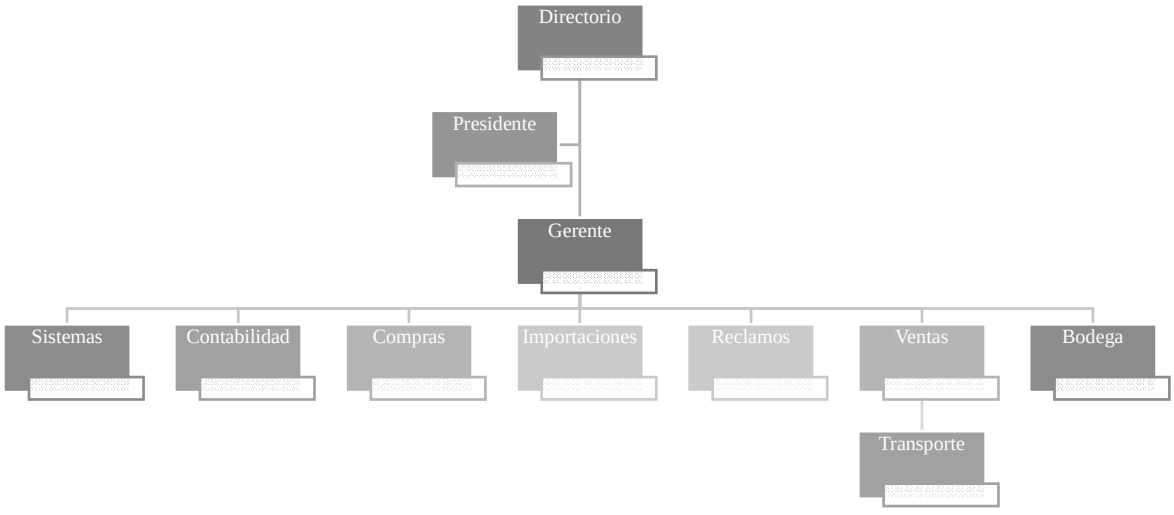
Transporte: Transportar los pedidos a los clientes y difundir la imagen de la empresa (Entrega de panfletos).

Orientación Gerencial y Técnica

En cuanto a la orientación gerencial se conoce que MADECO se centra en los empleados, es decir que vela por mantenerlos motivados y capacitados para que puedan desenvolverse de mejor manera. En cuanto a la orientación técnica la empresa ha establecido su enfoque en mejorar el entorno operativo-administrativo a través de servicios y productos suministrados por la unidad de sistemas, que aseguran el óptimo control de finanzas, estructura y recursos de la empresa mediante el uso de herramientas, investigación y desarrollo.

Estructura Organizacional

Actualmente se cuenta con 16 empleados, los cuales cumplen diferentes funciones de acuerdo a su cargo. La descripción gráfica es la siguiente:



Entorno Técnico

Se ha analizado a través de las entrevistas que el entorno técnico es de mucha importancia para la empresa puesto que la mayor parte de actividades y funciones dependen de la tecnología, en este caso: La comunicación entre sucursales, el sistema

interno que administra la información, etc. Además la unidad de sistemas trata de estar siempre a la vanguardia ofreciendo las mejores soluciones informáticas debido a la gran influencia del Sistema de TI en los procesos financieros, administrativos y técnicos que MADECO maneja.

En cuanto a los recursos técnicos, la empresa posee aproximadamente 48 equipos que trabajan para garantizar la funcionalidad de los procesos. Estos equipos se dividen en diferentes categorías, dispersas en las 4 localidades, entre estas tenemos: Servidor Master, Servidor de Respaldos, PC’s, impresoras, routers, escáneres, etc.

Anexo 2

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

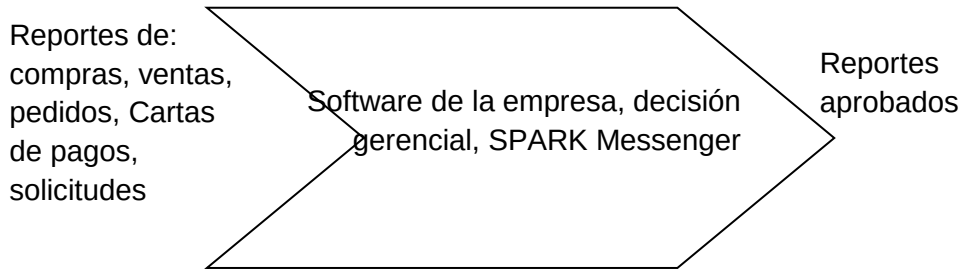
Persona entrevistada: Arq. Mauricio Heredia

Área: Gerencia

Fecha: 24 de Abril de 2013

1. **¿Cuál es el principal proceso dentro del área?**
   Gestión Administrativa (AD:G)

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



3. **¿Qué actividades identifica usted dentro del proceso**
   Realizar Revisiones

   Control de actividades

4. **¿Qué tareas componen a las actividades antes mencionadas?**
   1. REALIZAR REVISIONES

Revisar los reportes generados por cada departamento a través del sistema.

Comprobar que todos tengan los recursos necesarios para cumplimiento de labores.
Revisar si se han emitido solicitudes y aprobarlas si se considera necesario.

2. CONTROLAR ACTIVIDADES

Se mantiene contacto constante con todos los otros departamentos de la empresa vía llamadas telefónicas, en donde los encargados emiten su informe. Además se accede al sistema a realizar consultas sobre compras, ventas y pedidos.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: Ing. Mercedes Carrión

Área: Departamento de Ventas (AC:V)

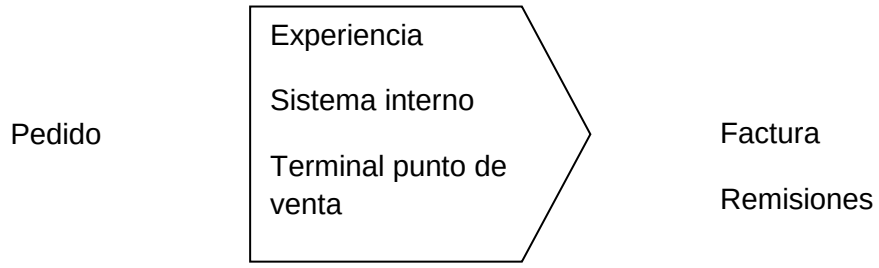
Fecha: 24 de Abril de 2013

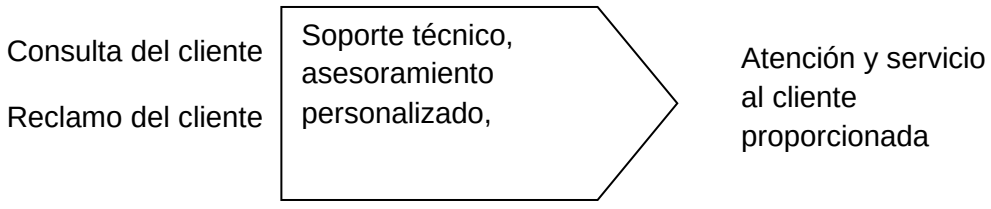
1. **¿Cuál es el principal proceso dentro del área?**

   Ventas

   Atención al cliente

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**





3. **¿Qué actividades identifica usted dentro del proceso**

   1.-Ventas:

   1.1.-Realizar los pedidos

1.2.-Registrar ventas al contado

1.3.-Registrar ventas a crédito

2.-Atención al cliente:

2.1.-Atender reclamos de los clientes

4. **¿Qué tareas componen a las actividades antes mencionadas?**

1.1. REALIZAR LOS PEDIDOS

Se recibe los pedidos por parte del cliente o se asesora durante la compra si el cliente no tiene claro lo que va a comprar, luego se verifica si hay en stock lo solicitado, para lo cual finalmente se emiten las facturas

1.2. REGISTRAR VENTAS AL CONTADO

Una vez entregada la factura al cliente, se recibe el dinero. En caso de ser a través de tarjeta de crédito se remiten al terminal punto de venta y se pasa la tarjeta de crédito, verificando que esta sea aprobada y que la tarjeta sea Dinners, American Express o VISA. Se emite la orden de entrega a bodega o se entrega el producto en caso de tenerlo en bodega chica.

1.3. REGISTRAR VENTAS A CRÉDITO

Para realizar las ventas a crédito, primero se revisa en el sistema si es un cliente fijo y si tiene o no deudas pendientes con la empresa, cuando la venta es realizada a crédito se procede al registro en cuentas pendientes en el sistema, luego se establece el tiempo y las condiciones de pago. Se firma una letra de cambio y se emite la orden de entrega a bodega o se entrega el producto en caso de tenerlo en bodega chica.

2.1. ATENDER RECLAMOS DE LOS CLIENTES

Se identifica el tipo de reclamo del cliente y se procede según sea necesario. En el caso de que el reclamo tenga que ver con la garantía del producto que se expendio, se realiza la llamada a la línea proveedora a la que se hizo la compra del producto y se solicita un técnico, al que se le proporciona los datos del cliente para que vaya a dar soporte. Finalmente se realiza una

llamada al cliente para saber si está satisfecho, caso contrario se repite el proceso o se comunica el caso a gerencia.

En el caso de que sea un reclamo en cuanto a un producto enviado que no ha sido especificado o que no conste dentro de la factura se cambia o se completa el pedido.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

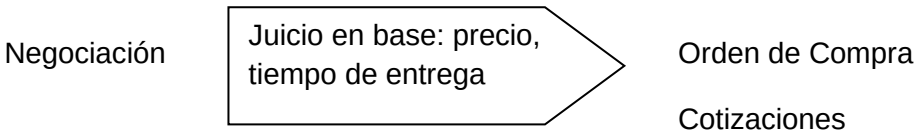
Persona entrevistada: Ing. Mercedes Carrión

Área: Departamento de Compras (AI:C)

Fecha: 24 de Abril de 2013

1. **¿Cuál es el principal proceso dentro del área?**
   Compras

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



3. **¿Qué actividades identifica usted dentro del proceso**
   Realizar las compras locales

4. **¿Qué tareas componen a las actividades antes mencionadas?**

   1. REALIZAR LAS COMPRAS LOCALES

   Se verifica semanalmente si el inventario solventa la demanda, en caso de que la bodega se esté quedando sin stock se busca en de la lista de proveedores las diferentes casas comerciales dentro del registro del sistema o en la guía telefónica para contactar con ellos, una vez hecho el contacto se realiza cotizaciones, si se llega a un acuerdo se elabora la orden de compra. Luego se recibe los productos y la nota de crédito. En caso de inconformidad se hace uso de la nota de crédito, caso contrario se acepta la factura y posteriormente se envía la factura a Contabilidad.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: Sr Luis Ayavaca

Área: Bodega (AC:B)

Fecha: 26 de Abril de 2013

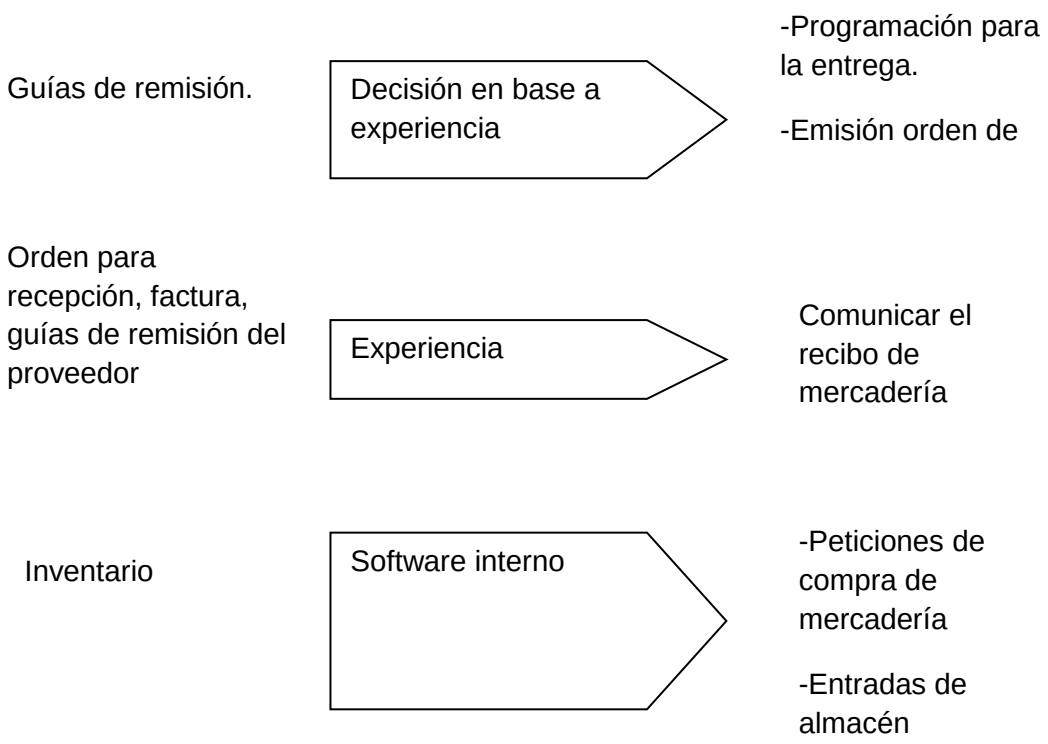
1. **¿Cuál es el principal proceso dentro del área?**

   Entrega de mercadería

   Recepción de mercadería

   Control de inventarios

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



3. **¿Qué actividades identifica usted dentro del proceso**

   Realizar entrega de mercadería

   Recibir la mercadería

   Realizar el control de inventario

4. **¿Qué tareas componen a las actividades antes mencionadas?**

   1. **REALIZAR ENTREGA DE MERCADERIA**

   El departamento de ventas emite una orden de entrega de productos a un determinado cliente. Se recepta la guía de remisión, se determina el tiempo de entrega y se envía al conductor los productos especificados en las guías de remisión, finalmente se entrega nuevamente la guía de remisión al conductor para el control de entrega.

   2. **RECIBIR MERCADERIA**

   Se acude a revisar que la mercadería este en buenas condiciones y que cumpla con lo estipulado en la guía de remisión del proveedor, en caso de cumplimiento se firma el documento, se recibe la factura

   3. **REALIZAR EL CONTROL DE INVENTARIO**

   Periódicamente se realizan revisiones de inventario para que haya coincidencia entre la mercadería física y la información del sistema, si existen inconvenientes o incongruencias son reportadas a gerencia. En caso de haber un stock limitado se realiza una solicitud de compra.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

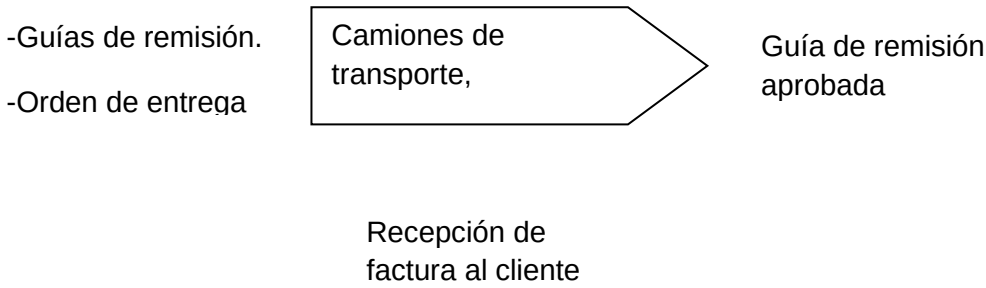
Persona entrevistada: Sr Luis Ayavaca

Área: Transporte (AC:T)

Fecha: 26 de Abril de 2013

1. **¿Cuál es el principal proceso dentro del área?**
   Entrega de pedidos

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



3. **¿Qué actividades identifica usted dentro del proceso**
   Realizar la entrega del pedido al cliente

4. **¿Qué tareas componen a las actividades antes mencionadas?**
   1. **REALIZAR ENTREGA DEL PEDIDO AL CLIENTE**

      Se recepta la guía de remisión y se carga el pedido en el camión, revisando que la mercadería este acorde a la guía de remisión. Se transporta el pedido al cliente, al momento de entregar la mercadería se solicita el comprobante de pago verificando si es el comprador, se pide al cliente que firme la guía de remisión como comprobante de recepción. Finalmente se lleva la guía de recepción firmada al jefe de bodega informando sobre el estado de la entrega

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: Ing. Marcos Orellana

Área: Departamento de Sistemas (AI:TI)

Fecha: 26 de Abril de 2013

1. **¿Cuál es el principal proceso dentro del área?**

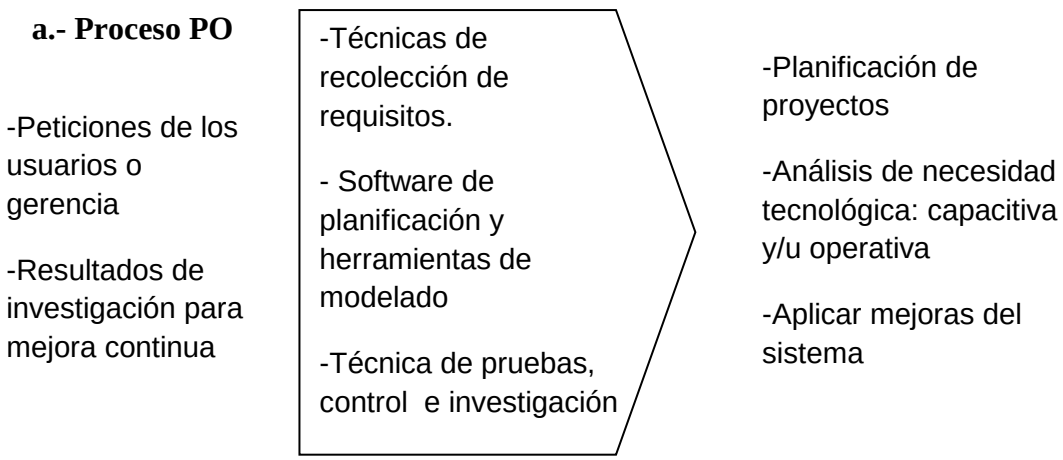
   1.-Proceso de cómputo y sistemas de información

   a.-Planificación y Organización de proyectos (PO)

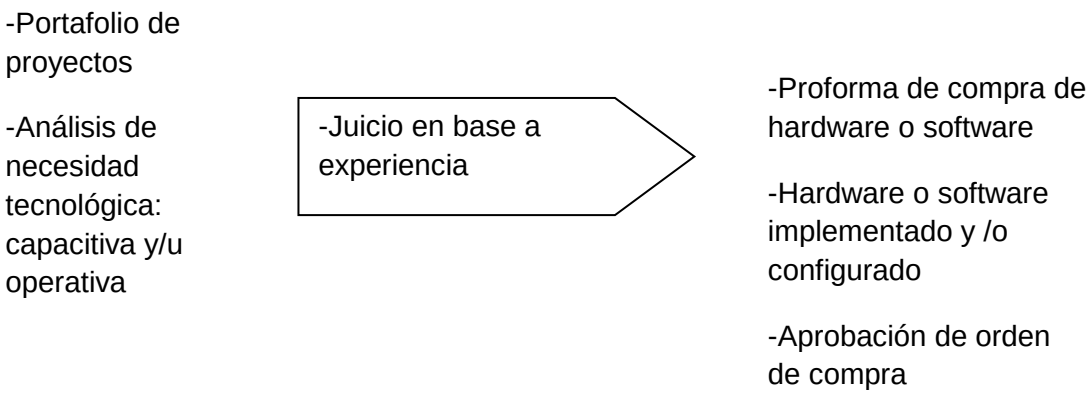
   b.-Adquirir e implementar herramientas tecnológicas (AI)

   C.-Desarrollo y entrega de aplicaciones. Soporte a usuarios (DS)

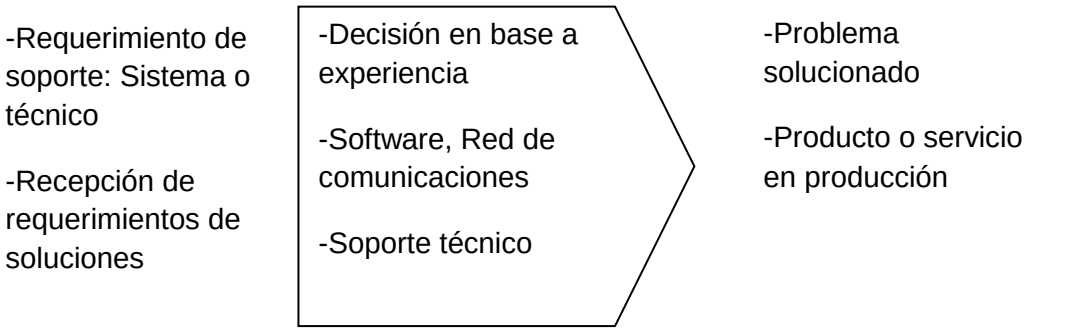
2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



B.-Proceso AI



C.-Proceso DS



3. ¿Qué actividades identifica usted dentro del proceso

1.-Planificar, organizar e implementar proyectos y la mejora de los mismos.

2.-Realizar planes de adquisición e implementación de tecnología.

3.-Realizar la entrega de servicios o productos y dar soporte si se requiere.

4. ¿Qué tareas componen a las actividades antes mencionadas?

1.-REALIZAR LA PLANIFICACION Y ORGANIZAR PROYECTOS

En el caso del sistema, se recibe el requerimiento de mejora o necesidad por parte de la gerencia, de los usuarios o del resultado de la investigación del departamento. Se analiza la factibilidad de implementación revisando la operación manual a sistematizar de los interesados a través de reuniones, se establecen prioridades entre requerimientos para proceder a su modelado, diseño de los módulos solicitados y se ejecuta el proyecto.

En el caso del hardware cuando se requiere, se realiza una propuesta de implementación para la mejora sistémica del negocio.

2.-REALIZAR PLANES DE ADQUISICION E IMPLEMENTACION DE TECNOLOGIA

La decisión sobre la adquisición de hardware o software depende de un análisis de necesidad para los usuarios o de la petición de la alta dirección. Dada la orden o la necesidad se realiza un análisis de mercado con las mejores opciones en productos. Se realizan varias proformas y se envían a la Gerencia para que sean analizadas y se elija la más conveniente.

En cuanto a implementación, se instala y configura el hardware o software adquirido o desarrollado por el departamento.

Al final de cada una de estas actividades se almacenan las proformas aprobadas como parte de la documentación y se comunica a Gerencia.

En cuanto a la entrega de productos adquiridos se recibe la aprobación de una de las proformas, se hace la negociación y finalmente la compra.

3.-REALIZAR LA ENTREGA DE SERVICIOS O PRODUCTOS Y DAR SOPORTE

Al hablar de soporte se recibe una llamada de cualquiera de los usuarios de las terminales, se analiza telefónicamente cual es el inconveniente o la petición. Se decide si es necesaria la intervención técnica presencial o caso contrario se guía al usuario para que resuelva el problema por sí mismo.

En el caso de la entrega de proyectos desarrollados, se planifica mediante prioridades la entrega de productos.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: Tania Heredia

Área: Presidencia (AD: P)

Fecha: 30 de Abril de 2013

1. **¿Cuál es el principal proceso dentro del área?**

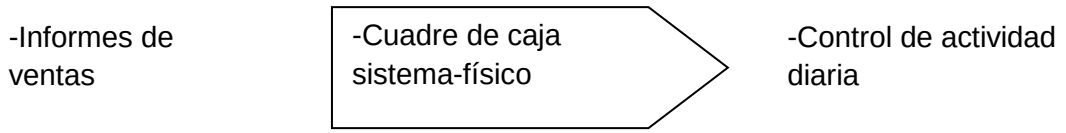
   1.-Auditoría y control de procesos centrales de negocio

   2.-Gestión Web

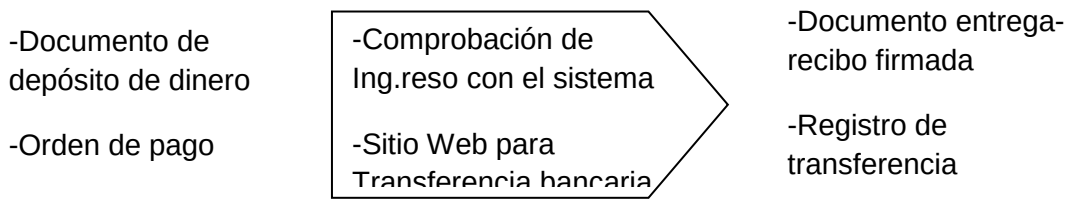
   3.-Coordinacion principal

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**

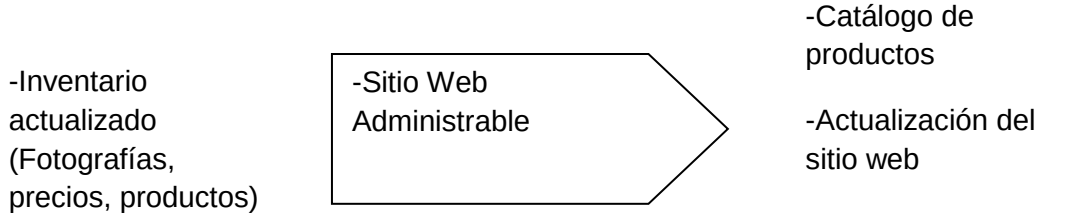
   1.-Auditoría y Control de procesos centrales de negocio



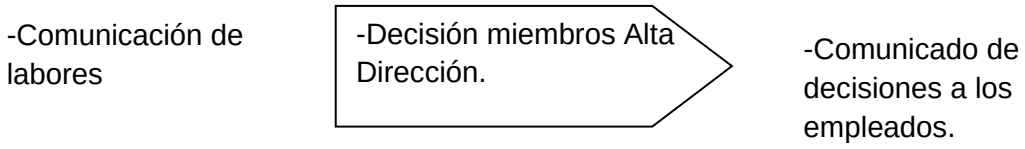
1.1.-Gestión Financiera



2.-Gestión Web



3.-Coordinacion principal



3. ¿Qué actividades identifica usted dentro del proceso

1.1.-Realizar la revisión de historiales de actividades de ventas en el sistema

1.2.-Realizar Gestión Financiera

2.1.-Administrar sitio Web

3.1.-Coordinar decisiones con Gerencia y Dirección Principal

4. ¿Qué tareas componen a las actividades antes mencionadas?

1.1.-REALIZAR LA REVISION DE HISTORIALES DE ACTIVIDADES DE VENTAS EN EL SISTEMA

Diariamente se revisan los registros de ventas a través del sistema. Se generan informes para verificar la actividad económica del día anterior. Se controla el nivel de ventas por local, los productos vendidos, etc. Se comunica a los miembros de la Alta Dirección.

1.2.-REALIZAR GESTIÓN FINANCIERA

Las vendedoras de cada sucursal realizan la entrega del dinero de las ventas del día. La presidenta se encarga de revisar y recibir el documento de depósito de dinero. Finalmente las dos partes firman un documento de entrega-recibo.

2.1.-ADMINISTRAR SITIO WEB

Se recibe información del inventario existente, stock, precio, fotografías y características del producto, el mismo que es Ing.resado en el sistema web guardado y publicado dentro del catálogo de productos. Así mismo si el sitio web necesita ser actualizado en cuanto a información de la empresa se modifica el contenido.

3.1.-COORDINAR DESICIONES CON GERENCIA Y DIRECCIÓN PRINCIPAL

Periódicamente se da la comunicación con la Gerencia y la Dirección Principal mediante mail, teléfono o reuniones para comunicación de labores: empleados, ventas y situación económica de la empresa. A través de la experiencia los miembros emiten decisiones que solucionan problemas o requerimientos. La decisión final es finalmente comunicada a los afectados.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: María Tapia

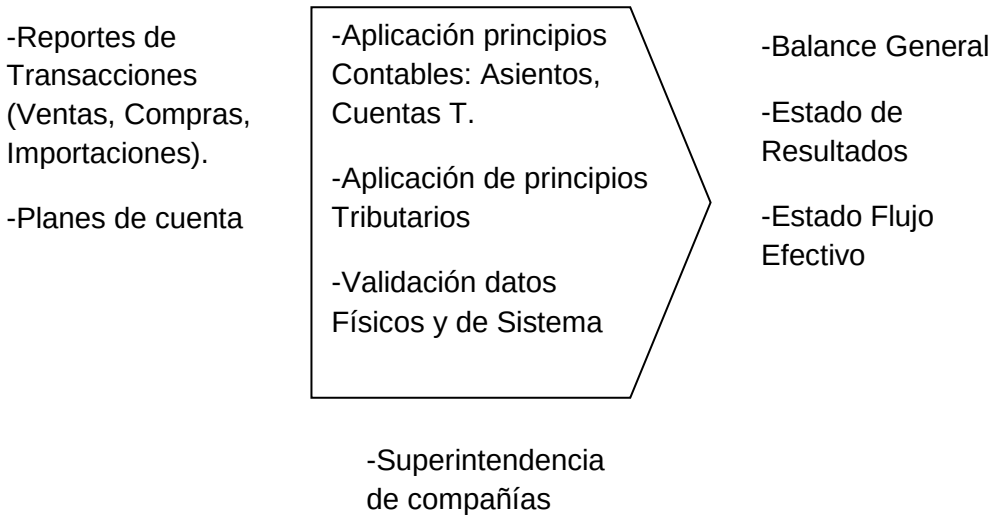
Área: Contabilidad (AI:F)

Fecha: 4 de Mayo de 2013

1. **¿Cuál es el principal proceso dentro del área?**

   Finanzas

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**



3. **¿Qué actividades identifica usted dentro del proceso**

   Realizar Contabilidad Interna

   Realizar Declaraciones Tributarias

4. **¿Qué tareas componen a las actividades antes mencionadas?**

   1. **REALIZAR CONTABILIDAD INTERNA**

Se receptan todos los documentos transaccionales de la empresa: Facturas de Proveedores, Facturas emitidas, retenciones, gastos de la empresa, etc. Posterior a ello se revisa en el sistema los reportes de ventas y facturación. Se hace una revisión para constatar que los datos del sistema cuadran con los datos físicos recibidos. Se aplican principios contables: Asientos, Cuentas T y finalmente se emiten Balances Generales, Flujos de Caja y Estado de resultados. Finalmente de comunican los resultados de los informes a Gerencia.

2. REALIZAR DECLARACIONES TRIBUTARIAS

Se recopilan todos los resultados de la actividad “Realizar contabilidad interna”, se organizan de manera que se puedan llenar los formularios del SRI declarando así los impuestos de la empresa. Se envían los documentos vía internet a través de los DIMM. Se informa del monto a cancelar y se comunica a Presidencia.

CUESTIONARIO MADECO

Este cuestionario permitirá identificar las actividades y tareas de los procesos principales del negocio

Empresa: MADECO Cía. Ltda.

Persona entrevistada: Alfonso Heredia

Área: Dirección General (AD:D)

Fecha: 4 de Mayo de 2013

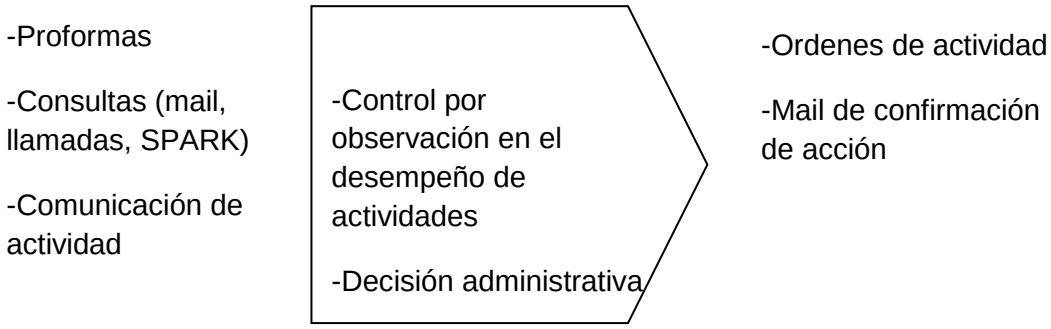
1. **¿Cuál es el principal proceso dentro del área?**

   1.-Proceso Dirección y Control.

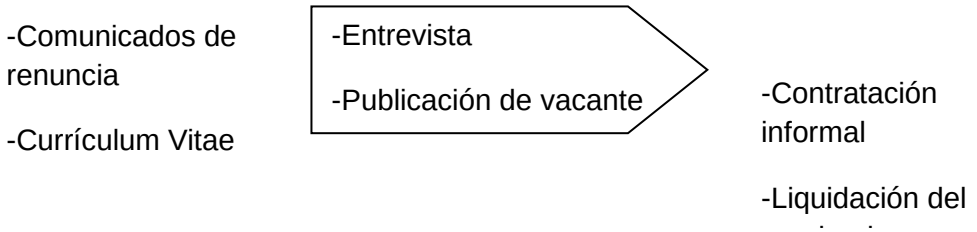
   2.-Gestión Recursos Humanos

2. **¿Qué input necesita cada proceso/qué output arroja el mismo?**

   1.-Proceso Dirección, Control y Coordinación



   2.-Gestión de Recursos Humanos



3. **¿Qué actividades identifica usted dentro del proceso**

   1.1.-Dirigir actividades diarias de los empleados

1.2.-Controlar actividades y necesidades

2.1.-Reclutamiento

2.2.-Desreclutamiento

2.3.-Capacitación

4. **¿Qué tareas componen a las actividades antes mencionadas?**

1.1.-DIRIGIR ACTIVIDADES DIARIAS DE LOS EMPLEADOS

Se provee de indicaciones a los empleados, sobre posibles compras, ventas, informes o de actividades que deben ser realizadas durante sus funciones. Esto es comunicado vía telefónica o correo electrónico. Se espera confirmación de recibo de indicaciones a los empleados.

1.2.- CONTROLAR ACTIVIDADES Y NECESIDADES

Se hace un control de desempeños de actividades del personal a través de visitas a las distintas sucursales o a través de las cámaras. En el caso de las visitas se hacen preguntas acerca de las funciones que cumplen o de la información que manejan. Si no se están cumpliendo regularmente sus obligaciones se hace un llamado de atención vía telefónica, personal o correo electrónico.

2.1.-RECLUTAMIENTO

Cuando un empleado es despedido o se da la necesidad por exceso de carga de trabajo inmediatamente se publican las vacantes en la prensa. Se receptan carpetas, las mismas que son analizadas verificando que cumplan el perfil que se desea cubrir, que vivan próximos a las instalaciones y que tengan experiencia en el área a la que van a trabajar. Se los entrevista para verificar su perfil psicológico y cultural. Se selecciona la persona que cumpla con los parámetros establecidos y se los contrata informalmente solo con los beneficios de ley durante 3 meses. Posteriormente si hay conformidad con el empleado después de los 3 meses recibe beneficios económicos superiores, mas comisiones dependiendo de su desempeño. Se dan indicaciones generales sobre

2.2.-DESRECLUTAMIENTO

Si uno de los empleados no cumple con sus obligaciones, no se desempeña o ha actuado provocando daños a la integridad de la empresa se lo despide. En caso de que el empleado no este conforme con su trabajo emite su comunicado a la Dirección sobre su decisión. Se liquidan los pagos con el empleado.

2.3.-CAPACITACIÓN

. Se planifican y financian las capacitaciones y el envió del personal a los cursos. Se comunica a los empleados sobre los cursos: Fecha, hora, lugar. Se verifica su asistencia.

Anexo 3

CONTROL:	Inventarios
FECHA DE EMISION:	15/02/2014
VERSION DOCUMENTO:	1.0

Ubicación	**Proceso**	**Tipo**	**Activo**	**Identificador**
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][easy]1	Mouse	4656A-VGPWM521
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][easy]2	Teclado VAIO	2012DJ4490
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][easy]3	Mouse	4356A-VGPWM521
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][pc] 16	Computador de oficina	SVJ202
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][peripheral][print]3	Impresora matricial	F7BG169051
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[HW][peripheral][print]4	Impresora laser	VNB3B23339
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[L] [buildIng.]2	Bodega Principal Gonzales	LB2PUI9LB3

			Suarez y Los Andes	
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][sub]1	Marcos Orellana	LB2PUI9PS1
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][sub]2	Katty Cabrera	LB2PUI9PS2
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ue]1	Jaime Pomaquiza	LB2PUI9PUE1
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ue]2	Isdrael Velezaca	LB2PUI9PUE2
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ue]3	Tania Heredia	LB2PUI9PUE3
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][u]1	Julia Orellana	LB2PUI9PUI1
[L] [buldog]2	Alta Dirección: Recursos Humanos	[P][ui]10	Arq. Mauricio Heredia	LB2PUI9PUI10
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]11	Rosana Jara	LB2PUI9PUI11
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]2	Claudio Sinchi	LB2PUI9PUI2
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]3	Tania Flores	LB2PUI9PUI3
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]4	Marcelo Paucar	LB2PUI9PUI4
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]5	Luis Ayavaca	LB2PUI9PUI5
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]6	María Tapia	LB2PUI9PUI6
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]7	Roberto Llivicota	LB2PUI9PUI7

[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]8	Ing. Mercedes Carrión	LB2PUI9PUI8
[L] [buildIng.]2	Alta Dirección: Recursos Humanos	[P][ui]9	Alfonso Heredia	LB2PUI9PUI9
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[SW][std] [office]8	Open Office	LB2PUI9SSO8
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[SW][std][browser]5	Firefox	LB2PUI9SSB5
[L] [buildIng.]2	Alta Dirección: Dirección y Control	[SW][std][os]18	WINDOWS 8	LB2PUI9SSO18
[L] [buildIng.]1	Alta Dirección: Gerencia	[HW][easy]4	Teclado	0N8WF8HE4
[L] [buildIng.]1	Alta Dirección: Gerencia	[HW][easy]5	Mouse	48729
[L] [buildIng.]1	Alta Dirección: Gerencia	[HW][pc] 9	Computador de oficina	7TTVCY1
[L] [buildIng.]1	Alta Dirección: Gerencia	[L] [buildIng.]1	Edificio 2 Gonzales Suarez y Guapondélig	LB1PUI10LB1
[L] [buildIng.]3	Alta Dirección: Gerencia	[L] [buildIng.]3	Edificio 1 Gonzáles Suarez frente al cementerio	LB1PUI10LB3
[L] [buildIng.]1	Alta Dirección: Gerencia	[SW][std][av]2	Kaspersky	000100057317DD75D3
[L] [buildIng.]1	Alta Dirección: Gerencia	[SW][std][browser]11	Firefox	LB1PUI10SSB11
[L] [buildIng.]1	Alta Dirección: Gerencia	[SW][std][os]4	WINDOWS 8	

[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]6	Teclado	XP136S809443
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]7	Teclado	02624978
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]8	Mouse GENIUS	121753303208
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]9	Mouse LENOVO	H5326HD102B
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][mid]1	Monitor LG	LB3PSU2HM1
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][mid]2	Monitor Samsung	D515MMDY705263E
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][pc] 13	Computador de oficina THINKCENTER	1S3264P3SMJ76L5Y
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][pc] 14	Computador de oficina SUPER POWER	LB3PSU2HP14
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][pc] 7	Computador de oficina	LB3PSU2HP7

[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][av]1	Kaspersky	000100057317DD75D3
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][browser]7	Firefox	LB3PSU2SSB7
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][office]2	Adobe Reader 9	LB3PSU2SSO2
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]11	WINDOWS 7	LB3PSU2SSI11
[L] [buildIng.]1	Compras	[D] [com]1	Órdenes de compra	LB1PUI8DC1
[L] [buildIng.]1	Compras	[D] [int]4	Cuadres caja	LB1PUI8DI4
[L] [buildIng.]1	Compras	[D] [int]5	Proformas	LB1PUI8DI5
[L] [buildIng.]1	Compras	[D] [int]6	Precios cerámica	LB1PUI8DI6
[L] [buildIng.]1	Compras	[HW][data]4	Terminal punto de venta	712256630
[L] [buildIng.]1	Compras	[HW][data]5	Terminal punto de venta	712436030
[L] [buildIng.]1	Compras	[HW][easy]10	Mouse	W66526607292
[L] [buildIng.]1	Compras	[HW][easy]11	Teclado	ZM6340010627

[L] [buildIng.]1	Compras	[HW][easy]12	Teclado	ZM3915301316
[L] [buildIng.]1	Compras	[HW][easy]13	Teclado	ZM6340010629
[L] [buildIng.]1	Compras	[HW][easy]14	Mouse	380334104242
[L] [buildIng.]1	Compras	[HW][easy]15	Mouse	123439506239
[L] [buildIng.]1	Compras	[HW][mid]3	Monitor	103TPVH31703
[L] [buildIng.]1	Compras	[HW][mid]4	Monitor	602MXJX18844
[L] [buildIng.]1	Compras	[HW][pc] 1	Computador de oficina	LB1PUI8HP1
[L] [buildIng.]1	Compras	[HW][pc] 2	Computador de oficina	LB1PUI8HP2
[L] [buildIng.]1	Compras	[HW][pc] 4	Computador de oficina	LB1PUI8HP4
[L] [buildIng.]1	Compras	[HW][peripheral][print]6	Impresora matricial	E8BY414377
[L] [buildIng.]1	Compras	[HW][peripheral][print]7	Impresora matricial	F7B6169052
[L] [buildIng.]1	Compras	[HW][peripheral][print]8	Impresora matricial	E83Y414253
[L] [buildIng.]1	Compras	[SW][std][av]4	NOD 32	LB1LB1PUI8SSA4
[L] [buildIng.]1	Compras	[SW][std][av]5	NOD 32	LB1LB1PUI8SSA5
[L] [buildIng.]1	Compras	[SW][std][av]6	NOD 32	LB1LB1PUI8SSA6

[L] [buildIng.]1	Compras	[SW][std][browser]10	Firefox	LB1LB1PUI8SSB10
[L] [buildIng.]1	Compras	[SW][std][browser]8	Firefox	LB1LB1PUI8SSB8
[L] [buildIng.]1	Compras	[SW][std][browser]9	Firefox	LB1LB1PUI8SSB9
[L] [buildIng.]1	Compras	[SW][std][office]5	Open Office	LB1LB1PUI8SSO5
[L] [buildIng.]1	Compras	[SW][std][office]6	Open Office	LB1LB1PUI8SSO6
[L] [buildIng.]1	Compras	[SW][std][office]7	Open Office	LB1LB1PUI8SSO7
[L] [buildIng.]1	Compras	[SW][std][os]17	Windows XP SP 3	NO ID/SIN LICENCIA
[L] [buildIng.]1	Compras	[SW][std][os]20	Windows XP SP 3	NO ID/SIN LICENCIA
[L] [buildIng.]1	Compras	[SW][std][os]9	Windows XP SP 3	NO ID/SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]16	Teclado	KBUSB0B28315102E900100
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][easy]17	Mouse	X80286301455
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][mid]5	Monitor	ZYJ2M4LD505536Y
[L] [buildIng.]3	Cómputo y Sistemas de	[HW][peripheral][print]13	Impresora matricial	E8BY396145

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][peripheral][print]2	Impresora matricial	61P1072860
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][browser]1	Firefox	LB3PSU1SSB1
[L] [buildIng.]3	Cómputo y Sistemas de información	[Aux] [cabling]1	Cableado UTP Cat 5	LB2PSU1AC1
[L] [buildIng.]3	Cómputo y Sistemas de información	[AUX] [furniture]1	Armario de manuales	LB3PSU1AF1
[L] [buildIng.]3	Cómputo y Sistemas de información	[AUX] [furniture]2	Armario de discos de respaldo	LB3PSU1AF2
[L] [buildIng.]3	Cómputo y Sistemas de información	[AUX] [furniture]4	Armario de dispositivos o herramientas varias	LB3PSU1AF4
[L] [buildIng.]3	Cómputo y Sistemas de información	[AUX] [furniture]5	RACK	LB3PSU1AF5
[L] [buildIng.]3	Cómputo y Sistemas de información	[AUX][UPS]1	UPS BATTERY	J50602004762
[L] [buildIng.]3	Cómputo y Sistemas de	[COM] [Internet]	Internet ETAPA	201.238.173.196

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM] [PSTN]1	Red de Telefonía IP	LB3PSU1CP1
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM] [radio]1	Radios	LB3PSU1CR1
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM] [radio]2	Red inalámbrica MADECO	LB3PSU1CR2
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM] [radio]3	Red inalámbrica ALERTHA	LB3PSU1CR3
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM][LAN]1	Red de área Local (LAN)	LB3PSU1CL1
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM][pp]1	Antenas parabólicas de conexión punto a punto	LB3PSU1CP1
[L] [buildIng.]3	Cómputo y Sistemas de información	[COM][sat]1	GPS	LB3PSU1CS1
[L] [buildIng.]3	Cómputo y Sistemas de información	[D] [conf]1	Datos de configuración de servidores	LB3PSU1DC1
[L] [buildIng.]3	Cómputo y Sistemas de	[D] [exe]1	Código fuente Sistema DOCS	LB3PSU1DE1

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[D] [exe]2	Código Ejecutable ASTERSIK	LB3PSU1DE2
[L] [buildIng.]3	Cómputo y Sistemas de información	[D] [test]1	Datos de pruebas	LB3PSU1DT1
[L] [buildIng.]3	Cómputo y Sistemas de información	[D] [voice]1	Voz IP	LB3PSU1DV1
[L] [buildIng.]3	Cómputo y Sistemas de información	[D] [vr]1	Base de datos	LB3PSU1DVR1
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][firewall]1	Firewall mikrotik	33B6025D1135
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][Switch]1	Switch HP	CN36BX12QC
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][Switch]2	Switch DLINK Monitor transaccional	DL0E15B000876
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][Switch]3	SWITCH HUAWEI	000FA3690550
[L] [buildIng.]3	Cómputo y Sistemas de	[HW][network][Switch]4	Switch LINKSYS	NO ID/ACCESO DIFICIL

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][Switch]5	Switch	NO ID/ACCESO DIFICIL
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]1	Access Point LINKSYS	LB3PSU1HNW1
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]2	Access Point	LB3PSU1HNW2
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]3	Access Point	LB3PSU1HNW3
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]4	Access Point LINKSYS	LB3PSU1HNW4
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]5	Access Point	LB3PSU1HNW5
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][network][wap]6	Access Point	LB3PSU1HNW6
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][pc] 12	Computador de oficina	0013206DD2E2
[L] [buildIng.]3	Cómputo y Sistemas de	[HW][peripheral][print]10	Impresora matricial	AE88033613C0

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW][peripherial][print]14	Impresora Matricial	CDUY108479
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW}[host]1	SERVIDOR HP	MXQ73502E2
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW}[host]2	SERVIDOR HP	MX231900CH
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW}[host]3	SERVIDOR HP	MX23110067
[L] [buildIng.]3	Cómputo y Sistemas de información	[HW}[host]4	SERVIDOR HP	MXQ3230134
[L] [buildIng.]3	Cómputo y Sistemas de información	[S][email]1	Correo	LB3PSU1SE1
[L] [buildIng.]3	Cómputo y Sistemas de información	[SI] [cd]1	CDROM	LB3PSU1SIC1
[L] [buildIng.]3	Cómputo y Sistemas de información	[SI] [dvd]1	DVD	LB3PSU1SID1
[L] [buildIng.]3	Cómputo y Sistemas de	[SW][std][app]2	VNC	LB3PSU1SSA2

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][app]3	Team Viewer	LB3PSU1SSA3
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][app]4	Putty	LB3PSU1SSA4
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][app]5	SPARK	LB3PSU1SSA5
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][dbms]1	Oracle Database 10g R2	15379961
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][dbms]2	Oracle Developer 10g	15379961
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][dbms]3	Erwin Data Modeler 7	NO ID/SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][dbms]4	PLSQL Developer 8	NO ID/SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][dbms]5	Oracle VM	LB3PSU1SSD5
[L] [buildIng.]3	Cómputo y Sistemas de	[SW][std][dbms]6	Oracle Application Server	LB3PSU1SSD6

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][email_client]1	Zimbra	LB3PSU1SSE1
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][file]1	Filezilla	LB3PSU1SSF1
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]1	Windows XP SP 3	NO ID/SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]10	WINDOWS 7	00371-OEM-8992671-00437
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]14	Linux 6.4 PROCESADOR 1	SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]15	Linux 6.4 PROCESADOR 2	SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]16	Linux 6.4 BLADE	SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][os]19	LINUX 4.7	SIN LICENCIA
[L] [buildIng.]3	Cómputo y Sistemas de	[SW][std][sub]1	Sistema DOCS	LB3PSU1SSS1

	información			
[L] [buildIng.]3	Cómputo y Sistemas de información	[SW][std][ts]1	ASTERISK	192.168.2.1
[L] [buildIng.]2	Ventas	[HW][easy]18	Teclado	ZCE730201612
[L] [buildIng.]2	Ventas	[HW][easy]19	Teclado	NO ID
[L] [buildIng.]2	Ventas	[HW][easy]20	Mouse	NO ID
[L] [buildIng.]2	Ventas	[HW][easy]21	Mouse	F66C80F5BRB03IM
[L] [buildIng.]2	Ventas	[HW][mid]6	Monitor	LS1S0SCD5-1
[L] [buildIng.]2	Ventas	[HW][mid]7	Monitor	HAL7H9NP334830Y
[L] [buildIng.]2	Ventas	[HW][pc] 17	Computador de oficina	GENERICO S/N
[L] [buildIng.]2	Ventas	[HW][pc] 3	Computador de oficina	GENERICO S/N
[L] [buildIng.]2	Ventas	[HW][peripherial][print]15	Impresora matricial	ETUY011002
[L] [buildIng.]2	Ventas	[SW][std][av]7	NOD 32	LB2PUI1SSA7
[L] [buildIng.]2	Ventas	[SW][std][browser]2	Firefox	LB2PUI1SSB2

[L] [buildIng.]2	Ventas	[SW][std][browser]6	Firefox	LB2PUI1SSB6
[L] [buildIng.]2	Ventas	[SW][std][office]9	Microsoft Office 2007	LB2PUI1SSO9
[L] [buildIng.]2	Ventas	[SW][std][os]3	Windows XP SP 2	SIN LICENCIA
[L] [buildIng.]2	Ventas	[SW][std][os]8	Windows XP SP 3	SIN LICENCIA
[L] [buildIng.]2	Bodega	[HW][easy]22	Teclado	BC2AACPUGM61
[L] [buildIng.]2	Bodega	[HW][easy]23	Mouse	F93AA0AN3UFAGJ3
[L] [buildIng.]2	Bodega	[HW][mid]8	Monitor	708NDFVDD411
[L] [buildIng.]2	Ventas	[HW][pc] 8	Computador de oficina	GENERICO S/N
[L] [buildIng.]2	Bodega	[SW][std][browser]4	Firefox	LB2PUI5SSB4
[L] [buildIng.]2	Bodega	[SW][std][office]10	Open Office	LB2PUI5SSO10
[L] [buildIng.]2	Bodega	[SW][std][os]7	Windows XP SP 2	SIN LICENCIA
[L] [buildIng.]3	Finanzas	[D] [adm]1	Facturas	LB3PUI6DA1
[L] [buildIng.]3	Finanzas	[D] [int]2	Roles	LB3PUI6DI2
[L] [buildIng.]3	Finanzas	[HW][easy]24	Teclado	GENERICO S/N
[L] [buildIng.]3	Finanzas	[HW][pc]15	Computador de oficina	00196065379729

			GATEWAY	
[L] [buildIng.]3	Finanzas	[HW][peripheral][print]1	Impresoras laser	vnb3d00219
[L] [buildIng.]3	Finanzas	[SW][std][browser]14	Firefox	LB3PUI6
[L] [buildIng.]3	Finanzas	[SW][std][office]1	Microsoft Office 2007	NO ID/SIN LICENCIA
[L] [buildIng.]2	Ventas	[HW][data]3	Terminal punto de venta	212555647
[L] [buildIng.]2	Ventas	[HW][easy]25	Teclado	B77420AGARR009
[L] [buildIng.]2	Ventas	[HW][easy]26	Mouse	W60861200844
[L] [buildIng.]2	Ventas	[HW][mid]9	Monitor	LS1SDSCDS-2
[L] [buildIng.]2	Ventas	[HW][pc] 5	Computador de oficina	GENERICO S/N
[L] [buildIng.]2	Ventas	[HW][peripheral][print]5	Impresora matricial	ETUY190615
[L] [buildIng.]2	Ventas	[SW][std][browser]3	Firefox	LB2PUI4SSB3
[L] [buildIng.]2	Ventas	[SW][std][office]11	Open Office	LB2PUI4SSO11
[L] [buildIng.]2	Ventas	[SW][std][os]5	Windows XP SP 3	SIN LICENCIA
[L] [buildIng.]3	Ventas	[D] [com]2	Letra de cambio	LB3PUI11DC2
[L] [buildIng.]3	Ventas	[D] [int]1	Registro de Tarjetas de	LB3PUI11DI1

			Crédito	
[L] [buildIng.]3	Ventas	[D] [int]7	Pagos Proveedores	LB3PUI11DI7
[L] [buildIng.]3	Ventas	[HW][data]1	Terminal punto de venta	712298165
[L] [buildIng.]3	Ventas	[HW][data]2	Terminal punto de venta	B00248D96
[L] [buildIng.]3	Ventas	[HW][easy]27	Teclado	ZM3915300243
[L] [buildIng.]3	Ventas	[HW][easy]28	Teclado	ZM3915300244
[L] [buildIng.]3	Ventas	[HW][easy]29	Mouse	GENERICO S/N
[L] [buildIng.]3	Ventas	[HW][easy]30	Mouse	4862A0V
[L] [buildIng.]3	Ventas	[HW][mid]10	Monitor	601MXYG10034
[L] [buildIng.]3	Ventas	[HW][mid]11	Monitor	919AB11CF329
[L] [buildIng.]3	Ventas	[HW][pc] 10	Computador de oficina	LB3PUI11HP10
[L] [buildIng.]3	Ventas	[HW][pc] 11	Computador de oficina	LB3PUI11HP11
[L] [buildIng.]3	Ventas	[HW][peripheral][print]11	Impresora matricial	F7BG169027
[L] [buildIng.]3	Ventas	[HW][peripheral][print]12	Impresora matricial	AEB038869B0
[L] [buildIng.]3	Ventas	[SI] [san]2	Pagos Proveedores	LB3PUI11SIS2

[L] [buildIng.]3	Ventas	[SI] [san]3	Registro de Tarjetas de Crédito	LB3PUI11SIS3
[L] [buildIng.]3	Ventas	[SW][std][browser]12	Firefox	LB3PUI11SSB12
[L] [buildIng.]3	Ventas	[SW][std][os]13	Windows XP SP 3	NO LICENCIA
[L] [buildIng.]3	Ventas	[SW][std][os]6	Windows XP SP 3	SIN LICENCIA
[L] [buildIng.]3	Finanzas	[AUX] [supply]1	Cintas	LB3PUI3AS1
[L] [buildIng.]3	Finanzas	[AUX][supply]3	Tóner	LB3PUI3AS3
[L] [buildIng.]3	Finanzas	[D] [int]3	ANEXOS	LB3PUI3DI3
[L] [buildIng.]3	Finanzas	[HW] [peripheral][scan]1	Scanner	C7K008946
[L] [buildIng.]3	Finanzas	[HW][easy]31	Teclado	123439S06282
[L] [buildIng.]3	Finanzas	[HW][mid]12	Monitor	LE15M9KY101135W
[L] [buildIng.]3	Finanzas	[HW][pc] 6	Computador de oficina	LB3PUI3HP6
[L] [buildIng.]3	Finanzas	[HW][peripheral][print]9	Impresora matricial	ALLY164459
[L] [buildIng.]3	Finanzas	[SI] [san]1	Balances	LB3PUI3SIS1
[L] [buildIng.]3	Finanzas	[SW][std][app]1	DIMM	LB3PUI3SSA1

[L] [buildIng.]3	Finanzas	[SW][std][av]3	NOD 32	LB3PUI3SSA3
[L] [buildIng.]3	Finanzas	[SW][std][browser]13	Firefox	LB3PUI3SSB13
[L] [buildIng.]3	Finanzas	[SW][std][office]3	Open Office	LB3PUI3SSO3
[L] [buildIng.]3	Finanzas	[SW][std][office]4	Microsoft Office 2007	SIN LICENCIA
[L] [buildIng.]3	Finanzas	[SW][std][os]12	WINDOWS 7	00359-OEM-9806534-79729
[L] [buildIng.]3	Finanzas	[SW][std][os]2	Windows XP SP 3	SIN LICENCIA
[L] [buildIng.]3	Alta Dirección: Presidencia	[COM][VPN]1	VPN	LB3PUI3CV1
[L] [buildIng.]3	Alta Dirección: Presidencia	[SW][std][www]1	Sitio Web	LB3PUI3SSW1

Elaborado por:	Fernanda Nivicela
Revisado y aprobado por:	
Número de Páginas:	10

Anexo 4

CONTROL:	Frecuencia de materialización de amenazas
FECHA DE ACTUALIZACION:	20/02/2014
VERSION DOCUMENTO:	v 1.0

	CODIGO	VULNERABILIDADES	FRECUENCIA DE OCURRENCIA
AMENAZAS NATURALES	[N.1]FUEGO	Falta de un sistema contra incendios	1
	[N.2] DANOS POR AGUA	Goteras	2
[i] AMENAZAS A INSTALACIONES	[I.1] FUEGO	Almacenamiento de productos inflamables sin adecuaciones	2
	[I.2] DANOS POR AGUA	Fugas de agua por daños de cañería	2
		Llaves de agua abiertas	
		Carencia de reglamento interno	

	[I.*] DESASTRES INDUSTRIALES	Instalaciones eléctricas no protegidas	3
		Carencia de protecciones físicas externas a las edificaciones	
	[I.3] CONTAMINACION MECANICA	Falta de planes de mantenimiento y limpieza de equipos	3
		Falta de reglamento interno	
	[I.5] AVERIA DE ORIGEN FISICO O LOGICO	Defectos de fabrica de los equipos	2
	[I.6] CORTE DEL SUMINISTRO ELECTRICO	Apagones por fallos del proveedor de energía eléctrica	3
	[I.7] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD	Falta de condiciones ambientales apropiadas para protección de los equipos	2
	[I.8]FALLO DEL SERVICIO DE COMUNICACIONES	Cableado de red inadecuado	3

		No disponer de un ISP adicional	
		Dispositivo de comunicaciones quemado	
		Dispositivos de comunicación mal configurados	
	[I.9] INTERRUPCION DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	Falta de equipamiento auxiliar en stock	2
		Falta de equipamiento auxiliar en stock	
		Falta de equipamiento auxiliar en stock	
	[I.10] DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	Falta de conservación de los soportes de información	2
		Mala manipulación de los soportes	
[E] ERRORES Y FALLOS NO INTENCIONADOS	[E.1] ERRORES DE LOS USUARIOS	Falta de capacitación del uso del sistema	3
		Falta de robustez del sistema	
		Falta de políticas de confidencialidad de información	
	[E.2] ERRORES DEL ADMINISTRADOR	Falta de inversión en horas de trabajo del personal	3

		Falta de plantillas de registro Falta de plan o políticas de registro de bitácoras	
	[E.3] ERRORES DE MONITORIZACION (LOG)	Falta de mecanismos de monitoreo	1
	[E.4] ERRORES DE CONFIGURACIÓN	Falta de manuales de configuración	2
		Falta de políticas de uso de aplicaciones y de información	
		Políticas incorrectas sobre el uso de passwords y proteccion de los equipos de comunicación	
	[E.7] DEFICIENCIAS EN LA ORGANIZACIÓN	Falta de capacitacion sobre seguridad de la información	2
		Falta de mecanismos de monitoreo del personal	
		Falta de políticas de uso correcto de telecomunicaciones	
		Falta de políticas de contratación	
		Carencia de control en la entrega de activos al caducar el contrato	

		Falta de motivación al personal	
	[E.8] DIFUSION DE SOFTWARE DANINO	Falta de políticas de uso de aplicaciones y de información	2
		Falta de control sobre la seguridad de la red	
		Falta de recursos de protección de los equipos de TI	
	[E.14] ESCAPES DE INFORMACIÓN	Falta de capacitación sobre seguridad de la información	3
		Carencia de mecanismos que controlen el envío y recepción de mensajes	
		Falta de políticas de uso de aplicaciones y de información	
		Falta de control de acceso físico a oficinas o salones restringidos	
	[E.16] INTRODUCCION DE INFORMACIÓN INCORRECTA	Sobrecarga de trabajo al personal	2
	[E. 17] DEGRADACION DE LA INFORMACIÓN	Carencia de planes de restitución de equipos	2
		Ubicación de los recursos en espacios desprotegidos	
		Falta de control del uso y buen funcionamiento de los equipos	

	[E.18] DESTRUCCION DE LA INFORMACIÓN	Falta de plan de respaldos de información critica	2
	[E.19] DIVULGACION DE INFORMACIÓN	Falta de capacitación sobre seguridad de la información	3
		Carencia de control en la entrega de activos al caducar el contrato	
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS SOFTWARE	Mala administración de llaves criptográficas	3
		Falta de validación de datos procesados	
		Mala Administración de la Base de Datos	
		Falta de políticas de uso de aplicaciones e información	
		Carencia de pruebas de software	
	[E.21] ERRORES DE MANTENIMIENTO/ACTUALIZACION SOFTWARE	Falta de planes de actualización	3
		Falta de control de software ilegal	
		La aplicación desactivada para actualizaciones	
		Falta de plan de mantenimiento	
	[E.23] ERRORES DE MANTENIMIENTO/ACTUALIZACION	Falta de un plan de mantenimiento de equipos de TI	3

	HARDWARE	Falta de plan de gestión y control de recursos vs requerimientos	
		Falta de planes de mantenimiento y limpieza de equipos	
	[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	Carencia de un plan de restitución de equipos	3
	[E.28] INDISPONIBILIDAD DEL PERSONAL	Falta de políticas de contratación	3
		Falta de un plan de contingencia en caso de ausencia	
[A] ATAQUES INTENCIONADOS	[A.4] MANIPULACION DE LA CONFIGURACIÓN	Segmentación de redes incorrecta	3
		Falta de políticas de uso de aplicaciones y de información	
		Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	
		Gestión de red inadecuada	

		Carencia de control en envío y recepción de mensajes	
		Falta de protección en redes públicas de conexión	
	[A.5] SUPLANTACION DE IDENTIDAD DEL USUARIO	Falta de capacitación sobre seguridad de la información	2
		Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	
		Falta de protección en redes públicas de conexión	
	[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	Gestión de red inadecuada	3
	[A.7] USO NO PREVISTO	Falta de mecanismos de monitoreo del personal	3
		Falta de políticas de uso correcto de telecomunicaciones	
	[A.8] DIFUSION DE SOFTWARE DANINO	Gestión de red inadecuada	3

		Falta de políticas de protección al equipo de TI	
	[A.11] ACCESO NO AUTORIZADO	Gestión de red inadecuada	3
	[A.13] REPUDIO	Carencia de mecanismos que controlen el envío y recepción de mensajes	2
	[A.14] INTERCEPTACION DE INFORMACIÓN	Carencia de mecanismos que controlen el envío y recepción de mensajes	3
		Gestión de red inadecuada	
		Falta de protección en redes públicas de conexión	
	[A.15] MODIFICACION DE LA INFORMACIÓN	Carencia de políticas de seguridad de uso de soportes de información externos	3
	[A.16] INTRODUCCION DE FALSA INFORMACIÓN	Carencia de políticas de seguridad de uso de soportes de información externos	2
	[A.17] CORRUPCION DE LA	Carencia de políticas de seguridad de uso de soportes de información	2

	INFORMACIÓN	externos	
	[A.18] DESTRUCCION DE LA INFORMACIÓN	Carencia de políticas de seguridad de uso de soportes de información externos	2
	[A.19] DIVULGACION DE INFORMACIÓN	Falta de motivación al personal	2
		Falta de mecanismos de monitoreo	
		Falta de capacitación sobre seguridad de la información	
	[A.22] MANIPULACION DE PROGRAMAS	Falta de políticas de uso de aplicaciones y de información	3
		Políticas incorrectas sobre el uso de passwords y protección de los equipos de comunicación	

	[A.24] DENEGACION DE SERVICIO	Uso complicado de interfaces	3
		Gestión de red inadecuada	
		Carencia de planes de restitución de equipos	
	[A.25] ROBO	Falta de control de acceso físico a oficinas o salones restringidos	2
		Ubicación de los recursos en espacios desprotegidos	
		Falta de control de uso y buen funcionamiento de los equipos	
	[A.26] ATAQUE DESTRUCTIVO	Falta de motivación al personal	2
		Falta de un plan de contingencia en caso de protestas civiles	
		Falta de un plan de contingencia en caso de protestas civiles	
	[A.28] INDISPONIBILIDAD DEL PERSONAL	Falta de políticas de contratación	3

	[A.29] EXTORSION	Falta de motivación al personal	1
	[A.30] ING.ENIERIA SOCIAL	Falta de capacitación sobre seguridad de la información	3
		Falta de mecanismos de monitoreo	
		Falta de políticas de uso correcto de telecomunicaciones	
		Falta de motivación al personal	

Anexo 5

CONTROL:	Valoración de amenazas
FECHA DE ACTUALIZACION:	20/02/2014
VERSION DOCUMENTO:	v 1.0

RESPONSABLE	Tipo	Disponibilidad	Integridad	Confidencialidad	Total
TANIA FLORES	[AUX] [supply]1	3	3	1	2
TANIA FLORES	[AUX][supply]3	3	3	1	2
MARIA TAPIA	[D] [adm]1	1	2	1	1
MARIA TAPIA	[D] [int]2	3	3	1	2
TANIA FLORES	[D] [int]3	5	5	1	4
TANIA FLORES	[HW] [peripheral][scan]1	2	1	1	1
MARIA TAPIA	[HW][easy]24	3	1	1	2
TANIA FLORES	[HW][easy]31	4	1	1	2
TANIA FLORES	[HW][mid]12	3	1	1	2
MARIA TAPIA	[HW][pc] 15	5	4	1	3
TANIA FLORES	[HW][pc] 6	1	3	1	2

MARIA TAPIA	[HW][peripheral][print]1	2	1	1	1
TANIA FLORES	[HW][peripheral][print]9	2	1	1	1
TANIA FLORES	[SI] [san]1	2	1	3	2
TANIA FLORES	[SW][std][app]1	2	2	2	2
TANIA FLORES	[SW][std][av]3	2	1	1	1
TANIA FLORES	[SW][std][browser]13	2	1	1	1
MARIA TAPIA	[SW][std][browser]14	2	1	1	1
MARIA TAPIA	[SW][std][office]1	3	1	1	2
TANIA FLORES	[SW][std][office]3	1	1	1	1
TANIA FLORES	[SW][std][office]4	3	1	1	2
TANIA FLORES	[SW][std][os]12	5	4	1	3
TANIA FLORES	[SW][std][os]2	1	3	1	2
TANIA HEREDIA	[COM][VPN]1	2	2	2	2
TANIA HEREDIA	[SW][std][www]1	4	4	5	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[Aux] [cabling]1	5	4	4	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[AUX] [furniture]1	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[AUX] [furniture]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[AUX] [furniture]4	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[AUX] [furniture]5	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[AUX][UPS]1	3	3	3	3
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM] [Internet]	3	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM] [PSTN]1	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM] [radio]1	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM] [radio]2	3	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM] [radio]3	3	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM][LAN]1	5	4	4	4

ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM][pp]1	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[COM][sat]1	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [conf]1	4	4	4	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [exe]1	3	4	4	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [exe]2	3	3	3	3
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [test]1	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [voice]1	1	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[D] [vr]1	5	5	5	5
ING. MARCOS ORELLANA	[HW][easy]16	1	1	1	1
ING. MARCOS ORELLANA	[HW][easy]17	1	1	1	1
ING. KATTY CABRERA	[HW][easy]6	1	1	1	1
ING. KATTY CABRERA	[HW][easy]7	1	1	1	1
ING. KATTY CABRERA	[HW][easy]8	1	1	1	1
ING. KATTY CABRERA	[HW][easy]9	1	1	1	1
ING. KATTY CABRERA	[HW][mid]1	1	1	1	1
ING. KATTY CABRERA	[HW][mid]2	1	1	1	1
ING. MARCOS ORELLANA	[HW][mid]5	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][firewall]1	3	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][Switch]1	4	3	3	3
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][Switch]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][Switch]3	3	3	3	3
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][Switch]4	4	4	4	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][Switch]5	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]1	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]3	1	1	2	1

ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]4	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]5	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][network][wap]6	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][pc] 12	1	2	2	2
ING. KATTY CABRERA	[HW][pc] 13	2	1	1	1
ING. KATTY CABRERA	[HW][pc] 14	1	1	1	1
ING. KATTY CABRERA	[HW][pc] 7	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][peripheral][print]10	1	1	1	1
ING. MARCOS ORELLANA	[HW][peripheral][print]13	1	1	1	1
ING. MARCOS ORELLANA	[HW][peripheral][print]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW][peripherial][print]14	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW}[host]1	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW}[host]2	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW}[host]3	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[HW}[host]4	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[S][email]1	2	2	3	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SI] [cd]1	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SI] [dvd]1	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][app]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][app]3	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][app]4	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][app]5	2	2	2	2
ING. KATTY CABRERA	[SW][std][av]1	2	1	1	1
ING. MARCOS ORELLANA	[SW][std][browser]1	2	1	1	1
ING. KATTY CABRERA	[SW][std][browser]7	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]1	5	5	5	5

ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]2	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]3	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]4	2	2	2	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]5	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][dbms]6	4	4	4	4
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][email_client]1	2	2	3	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][file]1	1	1	1	1
ING. KATTY CABRERA	[SW][std][office]2	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]1	1	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]10	2	1	1	1
ING. KATTY CABRERA	[SW][std][os]11	2	1	1	1
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]14	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]15	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]16	5	5	5	5
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][os]19	2	2	3	2
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][sub]1	3	3	4	3
ING. MARCOS ORELLANA, ING. KATTY CABRERA	[SW][std][ts]1	3	3	3	3
ALFONSO HEREDIA	[HW][easy]1	3	1	1	2
ALFONSO HEREDIA	[HW][easy]2	2	2	2	2
ALFONSO HEREDIA	[HW][easy]3	2	2	2	2
ALFONSO HEREDIA	[HW][pc] 16	2	2	2	2
ALFONSO HEREDIA	[HW][peripheral][print]3	1	1	1	1
ALFONSO HEREDIA	[HW][peripheral][print]4	2	2	2	2
ALFONSO HEREDIA	[L] [buildIng.]2	5	3	5	4
ALFONSO HEREDIA	[P][sub]1	1	2	1	1
ALFONSO HEREDIA	[P][sub]2	1	2	1	1

ALFONSO HEREDIA	[P][ue]1	1	2	1	1
ALFONSO HEREDIA	[P][ue]2	1	2	1	1
ALFONSO HEREDIA	[P][ue]3	1	2	1	1
ALFONSO HEREDIA	[P][ui]1	1	2	2	2
ALFONSO HEREDIA	[P][ui]10	2	2	2	2
ALFONSO HEREDIA	[P][ui]11	1	2	1	1
ALFONSO HEREDIA	[P][ui]2	1	2	1	1
ALFONSO HEREDIA	[P][ui]3	2	2	2	2
ALFONSO HEREDIA	[P][ui]4	1	2	2	2
ALFONSO HEREDIA	[P][ui]5	2	2	2	2
ALFONSO HEREDIA	[P][ui]6	2	2	2	2
ALFONSO HEREDIA	[P][ui]7	1	2	1	1
ALFONSO HEREDIA	[P][ui]8	2	2	2	2
ALFONSO HEREDIA	[P][ui]9	2	2	2	2
ALFONSO HEREDIA	[SW][std] [office]8	2	2	2	2
ALFONSO HEREDIA	[SW][std][browser]5	2	1	1	1
ALFONSO HEREDIA	[SW][std][os]18	2	2	2	2
LUIS AYAVACA	[HW][easy]22	1	1	1	1
LUIS AYAVACA	[HW][easy]23	1	1	1	1
LUIS AYAVACA	[HW][mid]8	3	1	1	2
LUIS AYAVACA	[HW][pc] 8	3	1	1	2
LUIS AYAVACA	[SW][std][browser]4	2	1	1	1
LUIS AYAVACA	[SW][std][office]10	1	1	1	1
LUIS AYAVACA	[SW][std][os]7	3	1	1	2
ING. MERCEDES CARRION	[D] [com]1	1	1	3	2
ING. MERCEDES CARRION	[D] [int]4	1	3	2	2

ING. MERCEDES CARRION	[D] [int]5	2	1	3	2
ING. MERCEDES CARRION	[D] [int]6	4	4	4	4
ING. MERCEDES CARRION	[HW][data]4	3	4	4	4
ING. MERCEDES CARRION	[HW][data]5	3	4	4	4
ING. MERCEDES CARRION	[HW][easy]10	3	1	1	2
ING. MERCEDES CARRION	[HW][easy]11	3	1	1	2
ING. MERCEDES CARRION	[HW][easy]12	3	1	1	2
ING. MERCEDES CARRION	[HW][easy]13	3	1	1	2
ING. MERCEDES CARRION	[HW][easy]14	3	1	1	2
ING. MERCEDES CARRION	[HW][easy]15	3	1	1	2
ING. MERCEDES CARRION	[HW][mid]3	3	1	1	2
ING. MERCEDES CARRION	[HW][mid]4	3	1	1	2
ING. MERCEDES CARRION	[HW][pc] 1	4	4	4	4
ING. MERCEDES CARRION	[HW][pc] 2	1	1	1	1
ING. MERCEDES CARRION	[HW][pc] 4	4	1	2	2
ING. MERCEDES CARRION	[HW][peripheral][print]6	4	4	4	4
ING. MERCEDES CARRION	[HW][peripheral][print]7	4	5	5	5
ING. MERCEDES CARRION	[HW][peripheral][print]8	4	4	4	4
ING. MERCEDES CARRION	[SW][std][av]4	2	1	1	1
ING. MERCEDES CARRION	[SW][std][av]5	2	1	1	1
ING. MERCEDES CARRION	[SW][std][av]6	2	1	1	1
ING. MERCEDES CARRION	[SW][std][browser]10	2	1	1	1
ING. MERCEDES CARRION	[SW][std][browser]8	2	1	1	1
ING. MERCEDES CARRION	[SW][std][browser]9	2	1	1	1
ING. MERCEDES CARRION	[SW][std][office]5	4	1	1	2
ING. MERCEDES CARRION	[SW][std][office]6	1	1	1	1

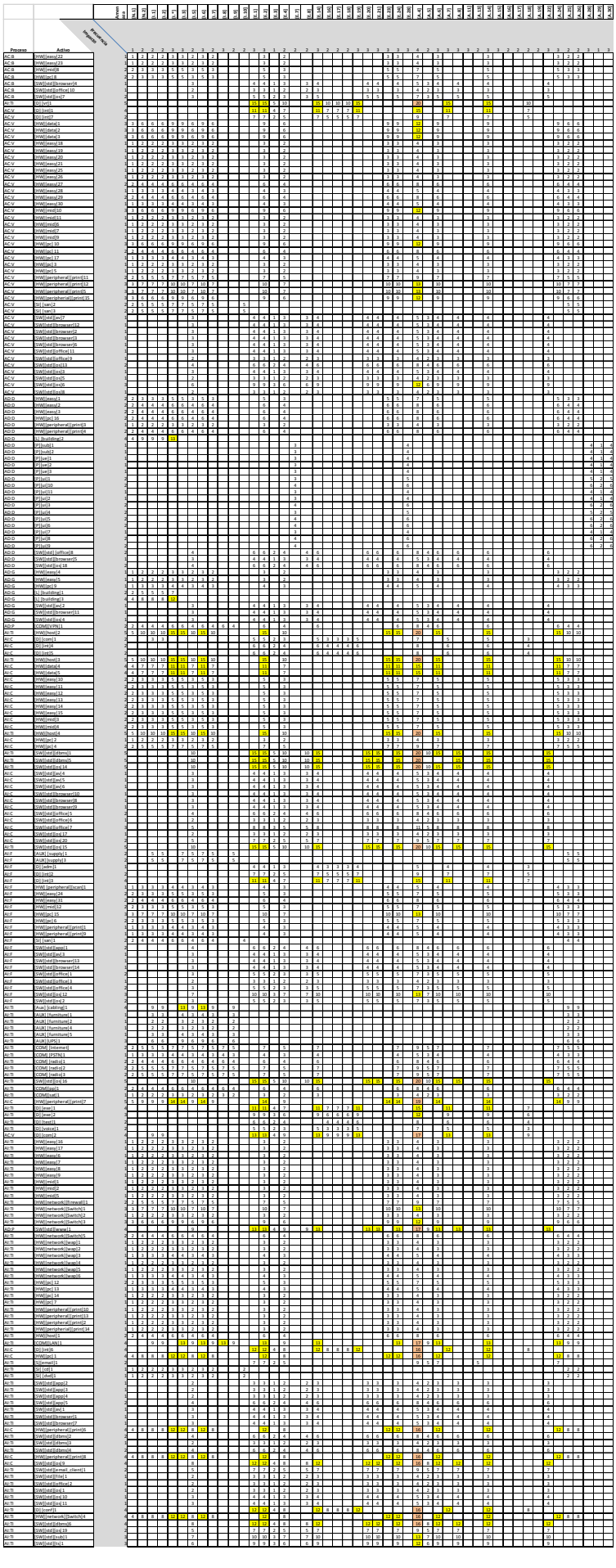
ING. MERCEDES CARRION	[SW][std][office]7	2	3	3	3
ING. MERCEDES CARRION	[SW][std][os]17	1	1	1	1
ING. MERCEDES CARRION	[SW][std][os]20	4	1	2	2
ING. MERCEDES CARRION	[SW][std][os]9	4	4	4	4
ROSANA JARA	[D] [com]2	4	5	4	4
ROSANA JARA	[D] [int]1	1	5	5	4
ROSANA JARA	[D] [int]7	3	3	1	2
ROSANA JARA	[HW][data]1	4	4	1	3
ROSANA JARA	[HW][data]2	4	4	1	3
MARIELA PAUCAR	[HW][data]3	4	4	1	3
JULIA ORELLANA	[HW][easy]18	1	1	1	1
JULIA ORELLANA	[HW][easy]19	1	1	1	1
JULIA ORELLANA	[HW][easy]20	1	1	1	1
JULIA ORELLANA	[HW][easy]21	1	1	1	1
MARIELA PAUCAR	[HW][easy]25	1	1	1	1
MARIELA PAUCAR	[HW][easy]26	1	1	1	1
ROSANA JARA	[HW][easy]27	4	1	1	2
ROSANA JARA	[HW][easy]28	2	1	1	1
ROSANA JARA	[HW][easy]29	4	1	1	2
ROSANA JARA	[HW][easy]30	2	1	1	1
ROSANA JARA	[HW][mid]10	4	4	1	3
ROSANA JARA	[HW][mid]11	1	1	1	1
JULIA ORELLANA	[HW][mid]6	1	1	1	1
JULIA ORELLANA	[HW][mid]7	1	1	1	1
MARIELA PAUCAR	[HW][mid]9	1	1	1	1
ROSANA JARA	[HW][pc] 10	3	4	2	3

ROSANA JARA	[HW][pc] 11	4	1	1	2
JULIA ORELLANA	[HW][pc] 17	2	1	1	1
JULIA ORELLANA	[HW][pc] 3	1	1	1	1
MARIELA PAUCAR	[HW][pc] 5	1	1	1	1
ROSANA JARA	[HW][peripheral][print]11	5	1	1	2
ROSANA JARA	[HW][peripheral][print]12	5	4	1	3
MARIELA PAUCAR	[HW][peripheral][print]5	4	3	3	3
JULIA ORELLANA	[HW][peripherial][print]15	4	3	2	3
ROSANA JARA	[SI] [san]2	3	3	1	2
ROSANA JARA	[SI] [san]3	3	3	1	2
JULIA ORELLANA	[SW][std][av]7	2	1	1	1
ROSANA JARA	[SW][std][browser]12	2	1	1	1
JULIA ORELLANA	[SW][std][browser]2	2	1	1	1
MARIELA PAUCAR	[SW][std][browser]3	2	1	1	1
JULIA ORELLANA	[SW][std][browser]6	2	1	1	1
MARIELA PAUCAR	[SW][std][office]11	2	1	1	1
JULIA ORELLANA	[SW][std][office]9	1	1	1	1
ROSANA JARA	[SW][std][os]13	4	1	1	2
JULIA ORELLANA	[SW][std][os]3	2	1	1	1
MARIELA PAUCAR	[SW][std][os]5	1	1	1	1
ROSANA JARA	[SW][std][os]6	3	4	2	3
JULIA ORELLANA	[SW][std][os]8	1	1	1	1
ARQ MAURICIO HEREDIA	[HW][easy]4	1	1	1	1
ARQ MAURICIO HEREDIA	[HW][easy]5	1	1	1	1
ARQ MAURICIO HEREDIA	[HW][pc] 9	1	1	2	1
ARQ MAURICIO HEREDIA	[L] [buildIng.]1	4	2	1	2

ARQ MAURICIO HEREDIA	[L] [buildIng.]3	5	5	2	4
ARQ MAURICIO HEREDIA	[SW][std][av]2	2	1	1	1
ARQ MAURICIO HEREDIA	[SW][std][browser]11	2	1	1	1
ARQ MAURICIO HEREDIA	[SW][std][os]4	1	1	2	1

Anexo 6

MATRIZ DE RIESGOS



Anexo 7

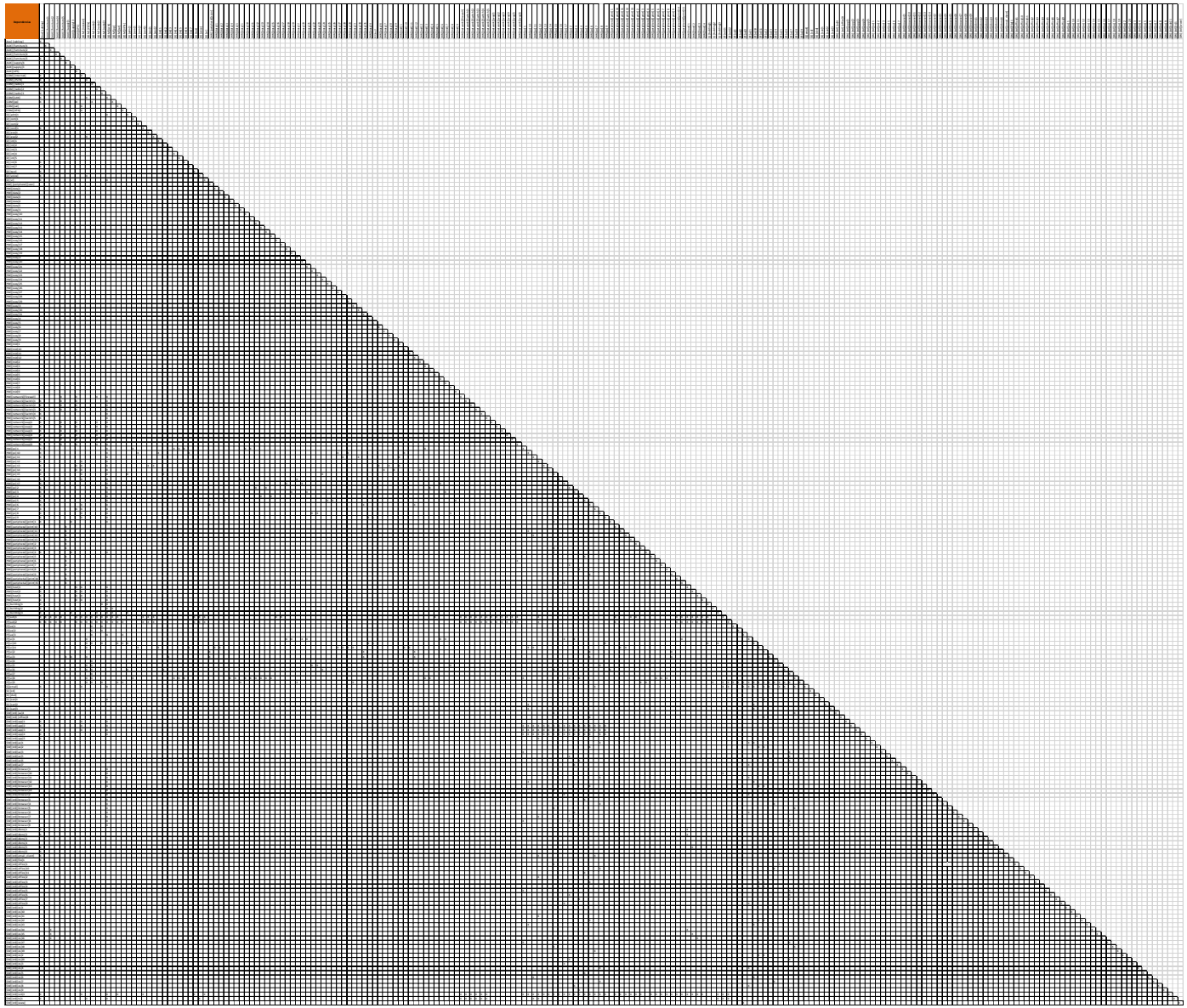
Checklist Plan de Pruebas	
Fecha inicio Proceso:	dd/mm/aaaa
Fecha Final del Proceso:	dd/mm/aaaa

Revisión	Parámetros	Cumplimiento
Revisión de documentación:	Descripción del problema	SI ☐ NO ☐
	Diagramas de clase	SI ☐ NO ☐
	Diagramas de Casos de Uso	SI ☐ NO ☐
	Restricciones y Limitaciones	SI ☐ NO ☐
Pruebas Unitarias Modulo 1	Búsquedas	SI ☐ NO ☐
	Validaciones	SI ☐ NO ☐
	Botones	SI ☐ NO ☐
	Consultas	SI ☐ NO ☐
	Visualización	SI ☐ NO ☐
Pruebas Unitarias Modulo 2	Búsquedas	SI ☐ NO ☐
	Validaciones	SI ☐ NO ☐
	Botones	SI ☐ NO ☐
	Consultas	SI ☐ NO ☐
	Visualización	SI ☐ NO ☐
Pruebas Unitarias Modulo N	Búsquedas	SI ☐ NO ☐
	Validaciones	SI ☐ NO ☐
	Botones	SI ☐ NO ☐
	Consultas	SI ☐ NO ☐
	Visualización	SI ☐ NO ☐
Pruebas de Integración	Ingreso de datos	SI ☐ NO ☐
	Modificación de datos	SI ☐ NO ☐
	Eliminación de datos	SI ☐ NO ☐
	Reportes de datos	SI ☐ NO ☐
Pruebas Funcionales o de Procedimientos	Procesos consistentes	SI ☐ NO ☐
	Cumplimiento requerimientos funcionales	SI ☐ NO ☐
	Cumplimiento parámetros de negocio	SI ☐ NO ☐
Pruebas de Sistema	Seguridad	SI ☐ NO ☐
	Usabilidad	SI ☐ NO ☐
	Estabilidad	SI ☐ NO ☐
	Rendimiento	SI ☐ NO ☐
	Concurrencia	SI ☐ NO ☐
	Interfaz	SI ☐ NO ☐
Pruebas de Regresión	Facilidad de uso	SI ☐ NO ☐
	Portabilidad	SI ☐ NO ☐
	Robustez	SI ☐ NO ☐
	otro	SI ☐ NO ☐

Revisado por:	
Aprobado por:	

Anexo 8

DEPENDENCIA ENTRE ACTIVOS



DOCTOR ROMEL MACHADO CLAVIJO,

SECRETARIO – ABOGADO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

DE LA UNIVERSIDAD DEL AZUAY,

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 11 de enero de 2013, conoció la petición de la señorita Miryam Fernanda Nivicela (código 46304) que denuncia su trabajo de tesis previa la obtención del Grado de Ingeniera de Sistemas, denominado: **"PLAN DE GESTIÓN DE RIESGOS PARA MADECO CÍA LTDA.".** Acogiendo el informe de la Junta Académica aprueba la denuncia y designa como Director de dicho trabajo al ingeniero Esteban Crespo Martínez y como miembros del Tribunal Examinador a los ingenieros Pablo Pintado Zumba y Pablo Esquivel León. De conformidad a las disposiciones reglamentarias la denunciante deberá presentar su trabajo de tesis en un plazo de **DIECIOCHO MESES** contados a partir de la fecha de aprobación, estos es hasta el 11 de JULIO de 2013.- Enmendado 4. Vale.

Cuenca, enero 15 de 2013

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

Oficio Nro. 014-2012-DIST-UDA

Cuenca, 10 de diciembre de 2012

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINSITRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 10 de diciembre de 2012, conoció el Proyecto de Tesis titulado "Plan de gestión de riesgos para MADECO Cia. Ltda", presentada por la estudiante Fernanda Nivicela, estudiante de la Escuela de Ingeniería de Sistemas y Telemática, previo a la obtención del título de Ingeniera de Sistemas y telemática.

La Junta considera que el diseño de tesis presenta una estructura teórica, metodológica y técnica objetiva y coherente, razón por la cual solicita, por su digno intermedio, el conocimiento y aprobación por parte del Consejo de Facultad.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda designar como Director de Tesis al Ing. Esteban Crespo, y como miembros del Tribunal al Ing. Pablo Pintado e Ing, Pablo Esquivel.

Atentamente,

Ing. Marcos Orellana Cordero
DIRECTOR ESCUELA DE INGENIERIA
DE SISTEMAS Y TELEMATICA

UNIVERSIDAD DEL AZUAY

Cuenca, 12 de diciembre de 2012

Ing.

Oswaldo Merchan

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

De mis consideraciones

Luego de haber cumplido con todos los créditos necesarios para poder realizar la tesis de graduación, yo Miryam Fernanda Nivicela con código 46304, alumna de Ingeniería en Sistemas y Telemática de la facultad de Administración solicito a usted me conceda la aprobación para poder comenzar el desarrollo de la tesis.

Por la favorable que se sirva dar a la presente le anticipo mi agradecimiento.

Atentamente,

Fernanda Nivicela

Edición autorizada de 20.000 ejemplares
Del 558.501 al 578.500
Nº 0568024

UNIVERSIDAD DEL AZUAY

Cuenca, 12 de Diciembre de 2012

Ingeniero

Oswaldo Merchán Manzano

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

Ciudad.

De mis consideraciones:

Yo, Ing. Esteban Crespo, profesor de la escuela de Sistemas, informo a Ud. que he procedido a revisar el diseño de Tesis presentado por la egresada Fernanda Nivicela, con el tema "PLAN DE GESTION DE RIESGOS PARA MADECO CIA. LTDA" como requisito previo a la obtención del título de Ingeniería de Sistemas, sobre el que emito el siguiente informe:

El proyecto tiene un alcance considerable dentro de la empresa Madeco, en el cual deberá realizar el levantamiento de activos de la información en todos los ámbitos que sugiere la norma española Magerit. Con esta información deberá identificar los riesgos y categorizar los impactos sobre cada activo en base a su grado de sensibilidad y disponibilidad, y diseñar políticas de Seguridad de la información para mitigar los riesgos identificados y garantizar la disponibilidad necesaria, aplicando el modelo de referencia ISO27001.

Por lo expuesto anteriormente, emito informe favorable y recomiendo su aprobación.

Muy atentamente:

Ing. Esteban Crespo, MBA, MCP

Edición autorizada de 20.000 ejemplares
Del 558.501 al 578.500 Nº 0568022

UNIVERSIDAD DEL AZUAY

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE INGENIERIA DE SISTEMAS Y TELEMATICA

DISEÑO DE TESIS

Tema:

Plan de Gestión de Riesgos para MADECO Cia. Ltda

Autor:

Miryam Fernanda Nivicela

Director:

Ing. Esteban Crespo M.

Cuenca, Ecuador

Miércoles 12 de diciembre de 2012

Edición autorizada de 20.000 ejemplares
Del 558.501 al 578.500 Nº 0568023

UNIVERSIDAD DEL AZUAY

Antecedentes y Justificación

Una de las problemáticas que afectan el desarrollo y buen funcionamiento de una empresa es la falta de un sistema de gestión de riesgos. Además también existen varios factores capaces de causar serios problemas financieros o de imagen con los clientes y proveedores de la empresa, ya sea por el incumplimiento en el tiempo de entrega de un producto o servicio o por que no se esté cumpliendo con la misión que inicialmente se planteó la empresa durante su creación.

Muchos de estos pueden ser el resultado de riesgos que no han sido neutralizados con un análisis y tratamiento previo de todos los activos de información así como los operacionales (en caso de haberlos). Por lo que se propone una solución viable para la continuidad del negocio previo a un desastre, en este caso un sistema de gestión de riesgos que sea capaz de mitigar todas las vulnerabilidades propensas a convertirse en riesgos para la organización, garantizando de esta manera disponibilidad, integridad y confidencialidad de la información de la empresa, es por eso que la siguiente tesis plantea seguir el modelo de seguridad de la información de la ISO 27001 que es la única norma certificable encargada de proporcionar parámetros y lineamientos que garanticen la seguridad de los activos de la empresa

Objetivos:

General

Crear un plan de gestión de riesgos de la información basada en la norma ISO 27001:2005, acorde a los controles y directrices que propone esta norma para la empresa Madeco Cía. Ltda.

Específicos

Realizar un levantamiento de activos de información de la empresa MADECO Cía. Ltda.

Analizar y clasificar los activos de la información en una jerarquía tal que denote la importancia que juega cada uno con respecto a la misión de la empresa

Identificar y analizar todas las amenazas posibles, su grado de impacto y el nivel de ocurrencia con el que se puedan suscitar.

Identificar y analizar las vulnerabilidades que pueden ser explotadas por las amenazas y convertirse en riesgos para la empresa

Generar un plan de seguridad para cumplir con los controles (ISO 27001:2005).

Alcance y delimitación

MADECO Cía. Ltda. es una empresa dedicada a la venta de materiales de construcción, está compuesta por cuatro almacenes de los cuales se va a analizar a la matriz principal y a una de las sucursales, para llegar a determinar vulnerabilidades que nos llevarán a establecer el tratamiento de riesgos adecuado como sugiere la norma ISO 27001.

Por tanto el plan de gestión de riesgos esta destinado a cubrir todas las brechas de seguridad que la empresa podría tener, describiendo como proteger cada uno de los activos de información y sus respectivos recursos utilizados (físicos y humanos) a través de los controles establecidos por la norma.

Referente teórico

ISO 27001

La información y recursos que una empresa posee son de vital importancia para el desarrollo y buen funcionamiento de la organización, por lo que deberían estar asegurados adecuadamente.

Para una adecuada gestión de seguridad de la información existe una norma británica estándar (ISO27001) que establece parámetros y lineamientos para la seguridad de información, está basado en la modalidad del ciclo Deming que consiste en: Planear, hacer, chequear y actuar. El objetivo principal de esta norma es preservar la integridad, confidencialidad y disponibilidad de la información. Su sistema se basa en la identificación de riesgos.

Fue aprobada en el año 2005 por la Organización Internacional para la Normalización (**ISO**) como norma certificable y es compatible con los estándares de calidad de producción que proporcionan las normas 9001 y 14001. Además debido a la naturaleza de la norma, esta puede ser aplicable a empresas de diferente tamaño e índole.

La aplicación del estándar en cada empresa varía según el alcance del sistema de gestión de seguridad establecido durante los pasos iniciales del periodo de implementación y al tamaño de la empresa.

MAGERIT

El creciente avance tecnológico de la información, así como las posibles amenazas naturales y humanas, dieron lugar a la creación de la metodología MAGERIT que permite minimizar los daños causados por los riesgos en recursos electrónicos, informáticos y telemáticos. Fue creado para atender específicamente la gestión de seguridad.

UNIVERSIDAD DEL AZUAY

Una empresa debe tener entero conocimiento acerca de cómo gestionar los riesgos de información, riesgos a los que podrían estar sometidos de no haberlos enfrentado y controlado previamente. La falta de control de esta naturaleza provoca que haya carencia de confianza en los sistemas de información. La ausencia de confianza limita a la organización de cumplir sus objetivos puesto que el tema mismo es inquietante para sus miembros.

Esta metodología está hecha para cualquier tipo de organización cuya información se encuentre informatizada. En caso de que los activos generados por este mecanismo sean valiosos, MAGERIT se encargará de valorarlos y a su vez protegerlos.

A través de esta herramienta también se pretende concientizar al gobierno de TI de la organización, de manera que puedan descubrir y planificar medidas oportunas para controlar los riesgos posibles. Además de planificar un entorno gestionado para futuras auditorias, certificaciones o acreditaciones, según sea el caso.

Esquema de contenidos

La tesis constara de los siguientes contenidos:

Capitulo 6: Políticas de seguridad

Edición autorizada de 20.000 ejemplares
Del 558.501 al 578.500
Nº 0568020

6.8.5. Seguridad en los procesos de desarrollo y soporte

6.8.6. Gestión de vulnerabilidad técnica

6.9. Gestión de incidente de seguridad de información

6.9.1. Reportar los eventos y debilidades de la información

6.9.2. Gestión de los incidentes y mejoras de seguridad de la información.

6.10. Cumplimientos

6.10.1. Cumplimiento de requisitos legales

6.10.2. Cumplimiento de las políticas y normas de seguridad y el cumplimiento técnico.

6.10.3. Consideraciones de auditoria de los sistemas de información

Conclusiones

Recomendaciones

Glosario

Bibliografía

Anexos

Cronograma

Tiempo	**MESES**					
Etapas y Actividades	1	2	3	4	5	6
Marco Teórico						
Situación actual de la empresa						
Levantamiento de activos						
Análisis de amenazas y vulnerabilidades						
Gestión de riesgos						
Políticas de seguridad						

Referencias Electrónicas

1. http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P8002922512936515509911&langPae=es&detalleLista=PAE_1276529683497133, 03 de septiembre 2012, Documentación oficial MAGERIT
2. HUIDROBO MOYA Jose, ROLDAN MARTINEZ David. http://books.google.com, 10 de septiembre 2012, Comunicaciones en redes WLAN: WiFi, VoIP, multimedia y seguridad
3. **ICA**,http://www.uazuay.edu.ec/bibliotecas/conectividad/mapa_conectividad/mapagene.html, 10 de septiembre 2012, Mapa de conectividad de internet
4. **UIT**,http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/MANUAL%20DE%20INDICADORES%20DE%20TELECOMUNICACIONES.pdf, 10 de septiembre 2012, Manual de indicadores de telecomunicaciones
5. **Sociedad de la información del Brasil**, http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Programa%20Sociedade%20da%20Informacao%20no%20Brasil%20Capitulo%201%20Espanol.PDF, 7 de septiembre de 2012, El Libro Verde de la Sociedad de la Información en Brasil
6. ICA, http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Telecentros%20Puente%20entre%20Tecnologia%20y%20Capital%20Social.pdf, 7 de septiembre de 2012, Un puente entre la tecnología y la sociedad
7. ICA,http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Wi-Fi%20en%20Educacion-Chile.pdf, 7 de septiembre de 2012, WI-FI EN LA EDUCACIÓN

Bibliografía

1. **Alberto G. Alexander**, *Diseño de un sistema de gestión de seguridad de información*, Editorial Alfaomega Colombiana S.A, Colombia, 2007, tomo I, Primera edición
2. **Jule Hintzbergen, Kees Hintzbergen, Andre Smulders, Hans Baars**, *Foundations of information Security*, Editorial Van Haren Publishing, United Kingdom, 2010, Segunda edición
3. **Alan Calder,Steve G. Watkins**, *Information Security Risk Management for ISO27001/ISO27002*, Editorial IT Governance Ltd 2007, United Kingdom, 2007, Primera edición
4. **GOMEZ, Alvaro**, *"Enciclopedia de la Seguridad Informática"*; (Spanish Edition)"; Alfaomega - Ra-Ma, 2011, segunda edicion

Edición autorizada de 20.000 ejemplares
Del 558.501 al 578.500
Nº 0568021

5. **EC-Council**; 2009; *"Ethical Hacking and Countermeasures: Attack Phases (Ec-Council Press Series: Certified Ethical Hacker)"*; Course Technology; 1 edition
6. **EC-Council**; 2009; *"Ethical Hacking and Countermeasures: Threats and Defense Mechanisms (Ec-Council Press Series: Certified Ethical Hacker)"*; Course Technology; 1 edition
7. **EC-Council**; 2009; *Computer Forensics: Hard Disk and Operating Systems (Ec-Council Press Series: Computer Forensics)"*; Course Technology; 1 edition (September 22, 2009)
8. **Barba Marti Antoni,** *Gestion de red,* Ediciones de la universidad Politecnica de Cataluña, España, 1999
9. **William Stallings,** *Comunicaciones y redes de computadores,* Editorial Prentice Hall, 2000
10. **Huidrobo Moya Jose, Roldan Martinez David,** *Comunicaicones en redes WLAN WiFi,VoIP, multimendia y seguridad,* Editorial Limusa, Mexico, 2006