DISEÑO DE UN MODELO DE ANÁLISIS Y DIAGNOSTICO DEL NIVEL DE MADUREZ EN SI PARA EN MIPYMES DE ASESORIA LEGAL Y OFICINAS DE ABOGADOS, COMO BASE PARA LA IMPLEMENTACION DE LA NORMA ISO27002.

TRABAJO DE GRADO

PARTICIPANTES

WILSON ARENALES GONZALEZ CÓD. 1412010614

LEIDY JOHANNA AVENDAÑO ROMERO CÓD. 1412010501

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

DISEÑO DE UN MODELO DE ANÁLISIS Y DIAGNOSTICO DEL NIVEL DE MADUREZ EN SI PARA EN MIPYMES DE ASESORIA LEGAL Y OFICINAS DE ABOGADOS, COMO BASE PARA LA IMPLEMENTACION DE LA NORMA ISO27002.

TRABAJO DE GRADO

PARTICIPANTES

WILSON ARENALES GONZALEZ CÓD. 1412010614

LEIDY JOHANNA AVENDAÑO ROMERO CÓD. 1412010501

Asesor(es)

GIOVANNY ANDRES PIEDRAHITA SOLORZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

AGRADECIMIENTOS

Quiero agradecer principalmente a Dios, a mi amado esposo, a mis queridos padres y al nuevo ser que está creciendo en mi ser, quienes me han dado la fortaleza de seguir adelante y han permitido, con todo su apoyo y colaboración, lograr esta nueva meta a nivel profesional.

Johanna.

Primero y como más importante, me gustarías agradecerle a Jesucristo y a DIOS que aparejo el tiempo y los recursos para realizar este nuevo estudio. También y muy importante agradecer a mi esposa, mis chiquitas y padres que son las personas que me brindaron el apoyo y la motivación para seguir adelante en los momentos difíciles.
Finalmente agradecer sinceramente al asesor y a cada uno a los tutores que en el transcurso de la especialización nos brindaron su esfuerzo, dedicación y conocimientos que fueron muy importante para nuestra formación como Especialista en seguridad de la información.

***Wilson A*.**

Tabla de contenido

Listado de tablas:

Listado de Figuras:

1. INTRODUCCIÓN

La necesidad de proteger la información, como uno de los activos más importantes, se ha convertido en uno de los desafíos para las empresas en los últimos tiempos. Se ha evidenciado que la falta de medidas para garantizar la confidencialidad, integridad o disponibilidad de la información, ha generado pérdidas económicas, legales y reputacionales en numerosas organizaciones de todo el mundo.

La información cada vez se está enfrentando a diferentes vulnerabilidades y amenazas que requieren atención para evitar serios impactos en las entidades[1]. Claramente el problema se agrava si las entidades no son conscientes de los riesgos a los que se exponen y las graves consecuencias que puede generar una deficiente gestión en Seguridad de la información.

Sumando a lo anterior, también surge un problema cuando las entidades consideran la seguridad solo desde el punto de vista de Tecnología, dejando a un lado otras buenas practicas que complementan y hacen que la seguridad sea integral, como es el caso de la seguridad física, políticas y procedimientos, sensibilización y capacitación, gestión de identidad, entre otros.

Todas estas y muchas otras problemáticas, son inherentes a cualquier tipo de organización. Sin embargo, cada empresa debe efectuar un análisis específico, dependiendo de su actividad económica, su misión y sus objetivos estratégicos. De acuerdo a lo anterior, para efectuar este ejercicio académico, se ha tomado la decisión de hacer un análisis detallado de las mipymes que desarrollan actividades de servicios profesionales de asesorías y representación legal.

[1] Informe sobre Amenazas a la Seguridad en Internet de Symantec Revela un Aumento en Ciberespionaje y un Crecimiento en los Ataques a Pequeñas Empresas. http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20130416_01

2. RESUMEN EJECUTIVO

2.1. Descripción general

Las Mipymes de representación y asesoría legal dentro de sus objetivos misionales tienen los siguientes: representan a los clientes en procesos judiciales, presentando pruebas y dando argumentos en la corte para respaldar la posición de sus clientes o como asesores, aconsejan a sus clientes sobre sus derechos y obligaciones legales, y sugieren el camino a tomar en temas comerciales y personales. Considerando lo anterior, se puede inferir se manipulan información sensible que requiere protección adecuada. Muchas de dichas entidades no cuentan con un sistema de seguridad que garantice que la información está salvaguardada.

Partiendo de esta premisa y otros criterios de análisis desarrollados en este trabajo, se hace necesario diseñar metodologías o guías de implementación inicial de un sistema de Seguridad de la Información, basado en los estándares mundiales y las mejores prácticas.

El presente trabajo se enfoca en el diseño de metodologías para identificar el nivel de madurez considerando los dominios y objetivos de control de la ISO 27002, identificar y clasificar activos de información, analizar y evaluar riesgos con el propósito de brindarles a las mipymes de asesoría legal un acercamiento a la seguridad y protección de la información desde diferentes frentes.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar una metodología de diagnóstico y análisis del nivel de madurez en seguridad de la información, aplicado específicamente a micro, pequeñas y medianas empresas dedicadas a asesorías y representación legal.

3.2. OBJETIVOS ESPECIFICOS

- Diseñar una metodología para diagnosticar el nivel de madurez para cada uno de los dominios de la norma ISO27002, aplicable a Mipymes de asesoría legal.

- Diseñar una metodología para la identificación y clasificación de los activos de información más críticos utilizados en Mipymes de asesoría legal.

- Proponer una metodología de análisis de riesgos de activos de información, en para Mipymes de asesoría legal.

- Proponer mecanismos de control de Seguridad de la Información acordes con la estructura y características específicas las Mipymes de asesoría y representación legal, basados en las buenas prácticas y dominios de la norma ISO27002 de 2013.

4. ALCANCE

El alcance de proyecto abarca desde el levantamiento de información y entrevistas específicas con expertos, hasta el diseño y propuesta de las metodologías de diagnóstico, identificación de activos de información, análisis de riesgos y propuestas de controles, basados en la norma ISO 27002 de 2013. Este modelo será aplicable a Mipymes de asesoría y representación legal.

5. RESULTADOS ESPERADOS DEL TRABAJO DE GRADO

Como resultado de este trabajo se espera presentar los siguientes entregables:

- ✓ Metodología de diagnóstico basada en la norma ISO 27002.
  - Levantamiento de información y diseño de metodología.
- ✓ Metodología para identificación y clasificación de activos de información
  - Levantamiento de información y diseño de metodología.
- ✓ Metodología de análisis y evaluación de riesgos de activos de información críticos.
  - Levantamiento de información y diseño de metodología.
- ✓ Aplicación piloto de las metodologías.

6. CRONOGRAMA

ACTIVIDADES	MES 1				MES 2			
	semana 1	semana 2	semana 3	semana 4	semana 1	semana 2	semana 3	semana 4
Levantamiento de información (entrevistas)								
Diseño de la metodología de diagnóstico basada en la norma ISO 27002. Aplicación de prueba piloto.								
Diseño de la Metodología para identificación y clasificación de activos de información. Aplicación de prueba piloto.								
Diseño de la Metodología de análisis y evaluación de riesgos de activos de información críticos. Aplicación de prueba piloto.								
Análisis final y propuesta de controles genéricos para Mipymes de asesoría legal								
Elaboración del documento								
Realización de ajustes								
Preparación de sustentación								

7. JUSTIFICACION

Con el propósito de hacer una aplicación práctica, realista y aterrizada de las teorías y conceptos analizados en la cátedra, se pretende diseñar una metodología de diagnóstico y análisis del nivel de madurez en seguridad de la información, aplicado específicamente a micro, pequeñas y medianas empresas dedicadas a asesorías y representación legal.

Con este proyecto se diseñarán metodologías y controles específicos para este tipo de empresas, con lo cual, por un lado se está contribuyendo con la generación de conocimiento y por otro lado, se puede contribuir para el crecimiento y fortalecimiento de las empresas.

Además, con la eventual aplicación de estas metodologías, se eliminaría el mito que dice que la seguridad de la información es solo para grandes empresas. Se debe generar conciencia de que en toda empresa (grande, pequeña, industrial, de servicios, etc.), la información siempre debe ser protegida y salvaguardada.

Por otro lado, analizando el sector económico en el que se aplicará este estudio, es decir el sector servicios, específicamente sector de asesoría y representación legal, se puede concluir que ejecutan actividades y operaciones con un alto volumen de información crítica y sensible a las que se deberían aplicar controles importantes para garantizar su confidencialidad, integridad y disponibilidad.

Además de lo anterior este proyecto toma especial importancia, dada la naturaleza de la sociedad colombiana, la cual se basa en un estado social de derecho. Lo anterior significa que se debe garantizar el cumplimiento de los derechos de los ciudadanos, y es por este motivo que se hace necesario que existan este tipo de organizaciones. Por consiguiente, todo aporte o contribución que se pueda hacer desde la academia, a los actores en procesos judiciales (juzgados, tribunales, abogados y oficinas de representación legal) redundará en una optimización de la administración de la justicia, logrando eficiencia y eficacia en la resolución justa de conflictos.

De igual forma, con el desarrollo de este proyecto se pretende fortalece la imagen y reputación del Politécnico gran Colombiano, demostrando su compromiso con el desarrollo y aporte a las organizaciones y al sector productivo, desde la academia y la investigación aplicada.

8. MARCO TEÓRICO Y REFERENTES

8.1. MARCO TEÓRICO

Seguridad de la Información

Se define como seguridad de la información a la protección de los activos contra pérdida, modificaciones no autorizadas, minimizando la probabilidad que se afecte la confidencialidad, integridad y disponibilidad por amenazas internas o externas, que pueden aprovechar vulnerabilidades de los activos afectando el funcionamiento directo y las condiciones de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella.

Garantizar un nivel de protección total es virtualmente imposible[2], la seguridad de la información en los entornos operativos no son cien por ciento seguros, es decir no existe un sistema seguro al ciento por ciento.

El propósito de la metodología de aseguramiento de la información está orientada a, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados por las compañías.

Principios de la seguridad de información

Dentro de los principios de la Seguridad de la Información, se tienen los siguientes:

- **CONFIDENCIALIDAD:** Criterio de información de COBIT que hace referencia a la protección de información sensible contra divulgación no autorizada.

- **INTEGRIDAD:** Criterio de información de COBIT que hace referencia a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- **DISPONIBILIDAD:** Criterio de información de CobiT que hace referencia a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas de un sistema para recuperarse rápidamente en caso de materialización de una amenaza que afecte la disponibilidad.

- **Controles** [1]
  Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

[2] ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información iso27000.es

- **Los objetivos de control** [1]: proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:

  - ✓ Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
  - ✓ Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
  - ✓ Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

- **ISO/IEC 27002** [2]**:** proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

  Dominio [2]: Agrupamiento lógico de procesos, a menudo se concibe como dominios de responsabilidad dentro de una estructura y encuadra en el ciclo de vida aplicable a los procesos de TI.

  Controles [2]: Los controles en la presente norma se pueden considerar como principios para la gestión de seguridad de la información y aplicable rector para la mayoría de las organizaciones. Los controles se explican en más detalle a continuación junto con una guía de implementación.

La versión de 2013 del estándar describe los siguientes catorce dominios principales de la ISO 27002:

- **Política Seguridad de la Información [3].**

  Este es un dominio está constituido por 1 objetivos de control y 2 controles[3]

  Objetivo: Un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

  El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores (legales de obligado cumplimiento, del sector al que pertenece la organización, de la propia organización de niveles superiores o más amplios) relacionadas.

- **Aspectos Organizativos de La Seguridad** [2]

[3] ISO/IEC 27001:2013 y 27002:2013

Este es un dominio que está constituido por 2 objetivos de control y 7 controles[3]

Objetivo:

El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.
Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades.

- **Seguridad Ligada a los Recursos Humanos** [2].

  Este es un dominio que está constituido por 3 objetivos de control y 6 controles[3]

  Objetivo:

  El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
  Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

- **Gestión de Activos** [2]

  Este es un dominio que está constituido por 3 objetivos de control y 10 controles[3]

  Objetivo:

  El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.
  Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información y asegurar que se aplica un nivel protección acorde, esto con el fin de minimizar los costos de gestión y tratamiento de la información de la compañía, de manera concordante con su nivel de clasificación teniendo cuenta:

  Responsabilidad sobre los activos. (Inventario de activos, Responsable de los activos y Acuerdos sobre el uso aceptable de los activos.)

  Clasificación de la información (Directrices de clasificación, Marcado y tratamiento de la información.)

- **Control de Accesos.** [2]

  Este es un dominio que está constituido por 4 objetivos de control y 14 controles[3]

  Objetivo:
  El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.
  Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

- **Cifrado.** [2]

  Este es un dominio que está constituido por 1 objetivo de control y 2 controles[3]

  Objetivo: El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

  La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

- **Seguridad Física y Ambiental**. [2]

  Este es un dominio que está constituido por 2 objetivos de control y 15 controles 3

  Objetivo:
  El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.
  El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

- **Seguridad de las operaciones** [2]**.**

  Este es un dominio que está constituido por 7 objetivos de control y 14 controles[3]

  Objetivo:
  El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas, equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

- **Seguridad de las Telecomunicaciones** [2]**.**

  Este es un dominio que está constituido por 2 objetivos de control y 7 controles[3]

  Objetivo:
  El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información.** [2]**.**

  Este es un dominio que está constituido por 3 objetivos de control y 13 controles[3]

  Objetivo:
  El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

  Aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

- **Relaciones con los Proveedores** [2]**.**

  Este es un dominio que está constituido por 2 objetivos de control y 5 controles[3]

  Objetivo:
  El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

- **Gestión de Incidencias** [2]**.**

  Este es un dominio que está constituido por 1 objetivo de control y 7 controles[3]

Objetivo:
El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

- **Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio** [2]**.**

  Este es un dominio que está constituido por 2 objetivos de control y 4 controles[3]

  Objetivo:
  El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

  Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

- **Cumplimiento** [2]**.**

  Este es un dominio que está constituido por 2 objetivos de control y 8 controles[3]

  Objetivo:
  El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.
  Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.
  El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

  El número total de controles suma 114 entre todas las secciones aunque cada organización debe considerar con anterioridad cuántos serán realmente implementados según sus propias necesidades.

- **MAGERIT [4]:** Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas elaborada por el Consejo Superior de Informática, cuya utilización promueve, como respuesta a la dependencia creciente de éstas (y en general de toda la sociedad) respecto a las Tecnologías de la Información.

- **Activos Tecnológicos**

  Según Magerit, recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Se pueden estructurar en cinco categorías: La gente (funcionarios, terceros y clientes), la información en cualquiera que sea su medio (oral, escrito, magnético), los procesos de la compañía, el hardware (equipos de

cómputo centrales y locales, redes de comunicación y redes eléctricas) y el software (programas aplicativos en general y sistemas operacionales).

- **Vulnerabilidad:**

  Según Magerit, se define como la ocurrencia real de materialización de una Amenaza sobre un Activo.

- **Administración de Riesgos**

  Según David McNamee, Proceso de gestión que sirve para determinar el nivel de riesgo existente para la información y definir un nivel de riesgo aceptable, adoptar medidas para reducir el riesgo al nivel aceptable y mantener dicho nivel de riesgo.

  - **Amenaza:** Acción, agente o evento que puede violar la seguridad de un entorno informático a partir de la explotación de fallos o puntos débiles (vulnerabilidades), y como consecuencia de ello, puede causar pérdidas o daños a los activos, afectando las actividades y el negocio de una organización; estas pueden ser emitidas de modo natural, intencional o involuntario como se muestra en la figura 1.

Figura 1 Amenazas

- **Análisis de Riesgos Informáticos**

  Es el estudio de la vulnerabilidades, amenazas probables eventos no deseados y los daños a los activos de información que se puedan causar al momento de materializarse.

- **Gestión De Riesgos** [5]
  Actividades coordinadas para dirigir y controlar una organización

- **Nivel De Riesgo** [5]
  Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad

- **Riesgo residual** [5]
  Riesgo restante después del tratamiento del riesgo.

8.2. MARCO CONTEXTUAL

El riesgo de seguridad de la información refleja la incidencia que ocasiona el compromiso de los activos de las compañías como la información, el hardware, el software, las personas y los procesos sobre los productos y servicios que ofrece el las pymes de asesoría legal que gestionan cobros de cartera de sus clientes.

Crear y dar mantenimiento a una metodología orientada que como objetivo es minimizar y administrar activos, riesgos, vulnerabilidades y controles en seguridad de la información a las pymes que no cuentan con recursos suficientes para implementar SGSI, es el apoyo o complemento que se puede brindar a la seguridad de la información de las compañías y a los usuarios finales.

La efectividad, la eficiencia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento y la confiabilidad de los datos para la toma de decisiones, manejo administrativo y operativo del negocio, son las premisas de la seguridad de la información que deben integrarse a la metodología propuesta.

El marco de trabajo a realizar documenta un nivel común de análisis de activos, riesgos en seguridad de la información, las estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de las pymes, causado por algún evento tecnológico no planeado se debe identificar, analizar y evaluar. Así mismo, se definiendo posibles estrategias de mitigación de riesgos más comunes en este tipo de compañías y así permitir minimizar la probabilidad de materialización de los riesgos.

El resultado de la metodología debe ser entendible para todas las personas involucradas y se debe expresarse en términos comunes, para permitir a los participantes conocer la importancia de la seguridad de la información y así alinear los riesgos a un nivel aceptable. Este marco de trabajo está sustentado en las mejores prácticas de tecnología y de seguridad de la información, conocidas e implementadas en el mundo como son ISO/IEC 27001:2013 y 27002:2013 que se han vuelto significativas debido a factores como:

- Mejorar productos, servicios y facilitar el controles de seguridad de los mismos.
- El creciente nivel de gasto en TI.
- La necesidad de satisfacer requerimientos legales en para empresas.
- Iniciativas para incluir la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas.
- Incremento de los riesgos informáticos

A continuación, se describen brevemente los documentos de referencia más relevantes para el proyecto [1]:

- “ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary”, provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI

- “ISO/IEC 27001:2013 - Information technology - Security techniques - Information Security Management Systems - Requirements”, es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.

- “ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security management” - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (14) cláusulas de control de la seguridad que contienen un total de treinta y cinco (35) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27001.

- La Ley Estatutaria 1581 de 2012[4] determina los principios a seguir en el manejo y tratamiento de datos personales, destacando el ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.:

  Principio de legalidad en materia de Tratamiento de datos: El tratamiento es una actividad reglada por lo tanto debe sujetarse a lo establecido en la ley y en las demás disposiciones.

  Finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.

  Libertad: El tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del titular.

  Veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

  Transparencia: En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del mismo, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

  Acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución.

  Seguridad: Los datos personales deben tratarse con las medidas técnicas, humanas y administrativas para dar seguridad a los registros de las bases de datos personales.

  Confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

[4] http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

9. DESCRIPCIÓN GENERAL DEL PROCESO DE LAS MYPIMES DE ASESORÍA Y REPRESENTACIÓN LEGAL.

Las mipymes de asesoría y representación legal, manejan un proceso principal que abarca desde el primer contacto con el cliente, pasando por el acompañamiento durante procesos judiciales, hasta gestionar y/o acompañar al cliente el proceso de cobro, para finalizar con la facturación y pago de honorarios.

Para el levantamiento de este procedimiento, se efectuaron entrevistas con expertos, los cuales tienen amplia experiencia profesional en empresas de este tipo. A continuación se presenta de forma estructurada el diagrama general del proceso, en el cual se pueden identificar las etapas, actividades y las posibilidades que se presentan durante la representación legal de un cliente en un proceso judicial.

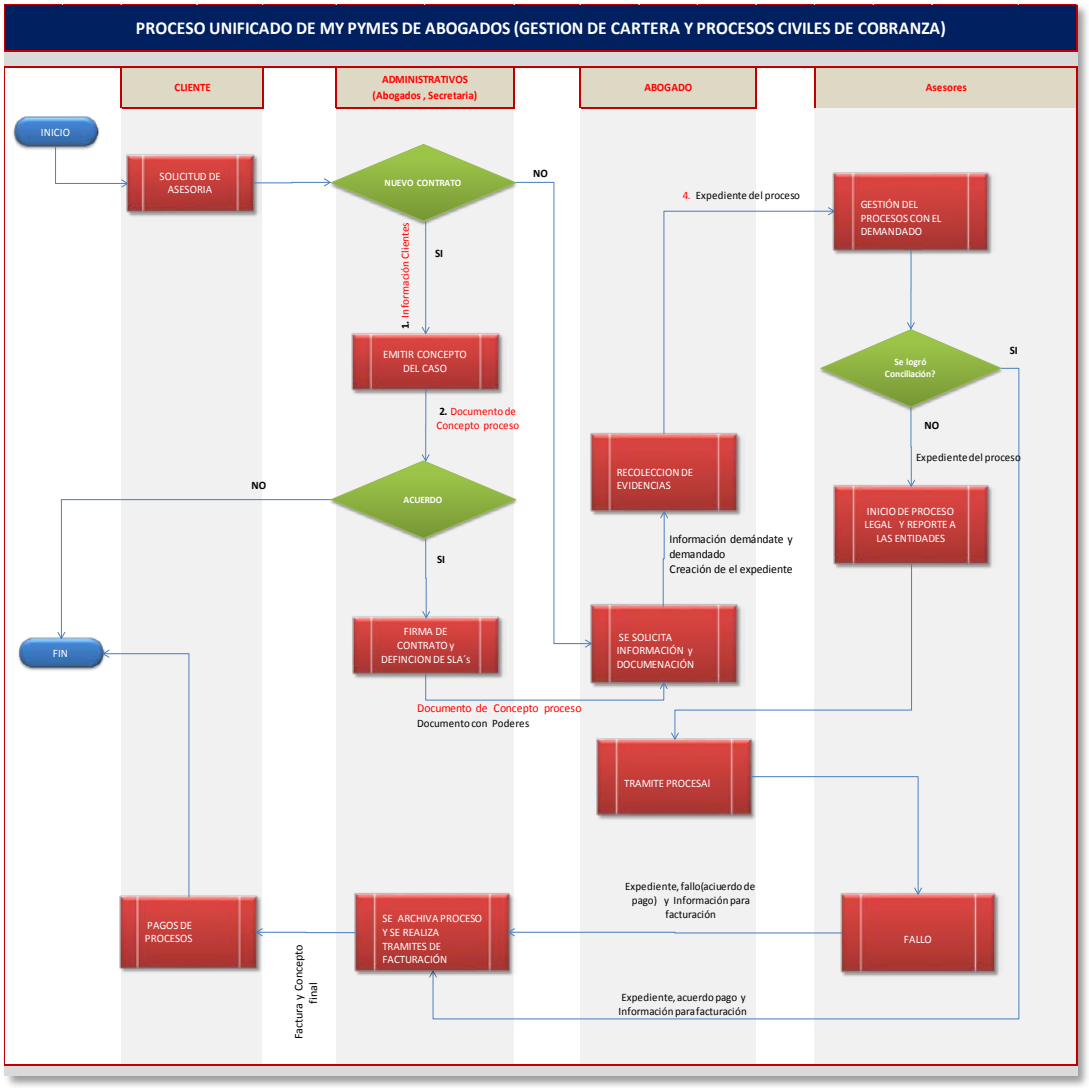


Figura 2 Proceso de las compañías

10. ESTRUCTURA DEL MODELO DE ANÁLISIS Y DIAGNÓSTICO.

Una vez identificado el proceso general de este tipo de empresas, se procede a diseñar y estructurar el modelo de diagnóstico y análisis, el cual es el foco principal de este proyecto.

El modelo que se presentará en los próximos capítulos, se basará en un análisis sistemático teniendo en cuenta los componentes más significativos a la hora de fortalecer la Seguridad de la información. A continuación se resumen dichos componentes, los cuales serán estudiados y desarrollados en el siguiente orden:

- Metodología de diagnóstico basada en la norma ISO 27002.

En primer lugar, para poder diseñar y aplicar el modelo, es necesario realizar un diagnóstico adecuado del nivel de madurez en SI para la empresa que quiera aplicar este estudio. En este sentido, la primera etapa consiste en diseñar una metodología de diagnóstico y aplicarla con una prueba piloto.

- Metodología para identificación y clasificación de activos de información.

Considerando que los activos de información son de gran valor para todas las organizaciones, el siguiente paso es identificarlos y clasificarlos de tal manera que se pueda determinar cuáles son los más críticos. Estos activos críticos tendrán una mayor importancia a la hora de adelantar el análisis de riesgos.

- Metodología de análisis y evaluación de riesgos de activos de información críticos.

Teniendo en cuenta las vulnerabilidades y amenazas a las que se pueden enfrentar los activos de información, en esta etapa se hará un análisis de riesgos para cuantificar su criticidad y nivel de riesgo. Con el anterior análisis, se obtiene una base importante para el diseño y la propuesta de controles adecuados y efectivos

- Análisis experto: diseño de controles y recomendaciones.

En este apartado, considerando las etapas anteriores, se concluirá el análisis con el diseño y la propuesta de controles específicos que puedan ser aplicables en Mipymes de asesoría y representación legal.

El siguiente es el diagrama explicativo del modelo de análisis y diagnóstico.

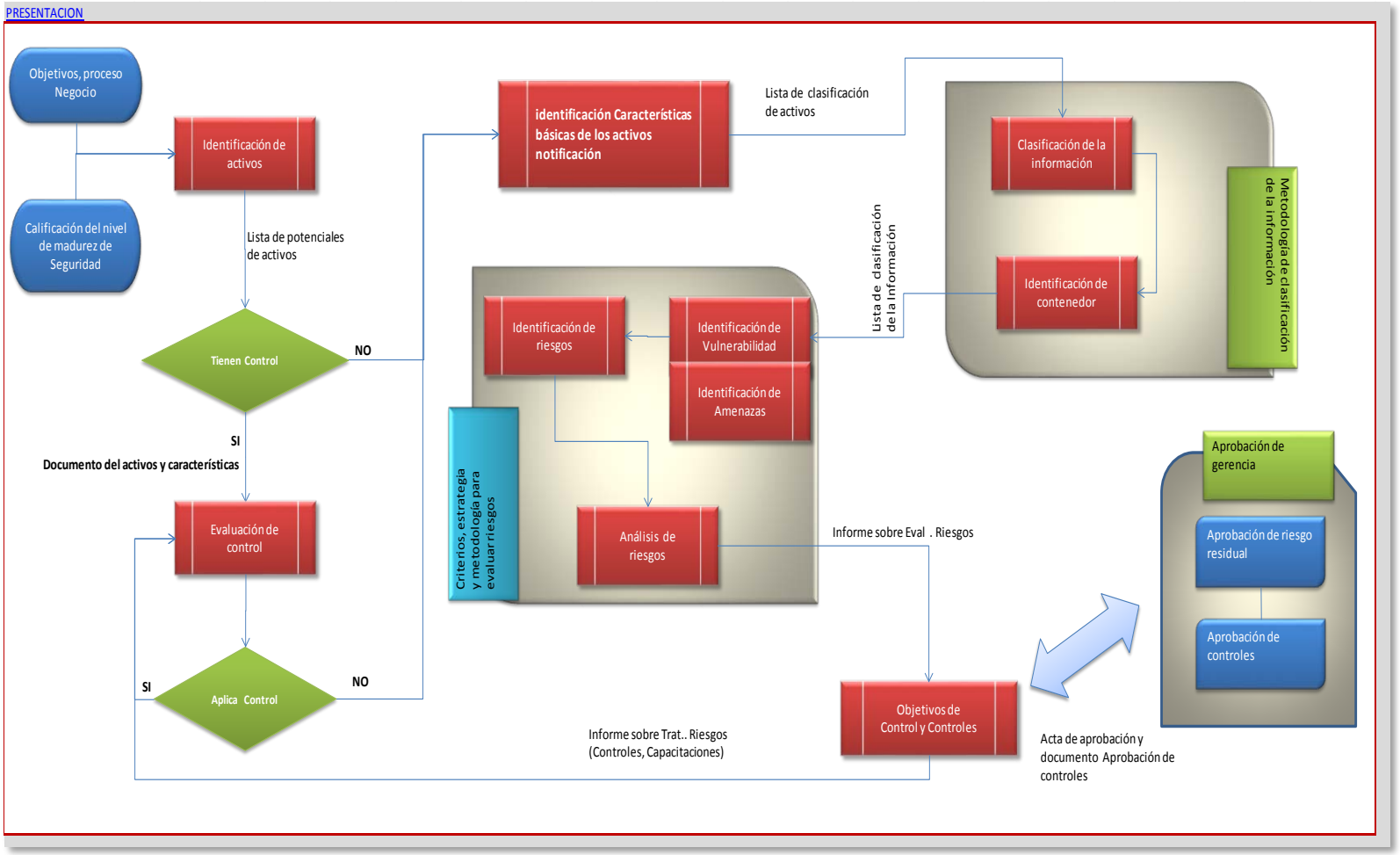


Figura 3 Modelo de análisis

11. METODOLOGÍA DE DIAGNÓSTICO BASADA EN LA NORMA ISO 27002

Como punto de partida, para identificar el nivel del grado de madurez en Seguridad de la Información, se plantea una metodología basada en los objetivos de control de la norma ISO 27002 y en el modelo planteado en COBIT 4.1.

Dicha metodología permite evaluar por dominio y objetivo de control, el nivel en el que se encuentra la entidad considerando diferentes escalas. Lo anterior permitirá que las entidades determinen qué deben fortalecer y así poder tomar decisiones en pro del mejoramiento de la Seguridad de la Información.

11.1. PLANTILLA DE EVALUACIÓN - DIAGNOSTICO

EVALUACIÓN DE APLICABILIDAD: Considerando los 14 dominios, 35 objetivos de control y 114 controles de la ISO 27002 de 2013, se realizó un análisis de la aplicación de cada uno en las entidades objeto de estudio.

Teniendo en cuenta lo anterior, se realizó una depuración de los controles por dominio que aplican a las mipymes de asesoría y representación legal para efectuar la evaluación. Ver tabla No. 2

DOMINIO	OBJETIVOS DE CONTROL		APLICA	OBSERVACIONES
POLÍTICAS DE SEGURIDAD	**5.1**	**Directrices de la Dirección en seguridad de la información.**		
	5.1.1	Conjunto de políticas para la seguridad de la información.	SI	
	5.1.2	Revisión de las políticas para la seguridad de la información	SI	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**6.1**	**Organización interna.**		
	6.1.1	Asignación de responsabilidades para la segur. de la información	SI	
	6.1.2	Segregación de tareas	SI	
	6.1.3	Contacto con las autoridades.	SI	
	6.1.4	Contacto con grupos de interés especial.	SI	
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	
	6.2	**Dispositivos para movilidad y teletrabajo**		
	6.2.1	Política de uso de dispositivos para movilidad.	SI	
	6.2.2	Teletrabajo.	SI	
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**7.1**	**Antes de la contratación.**		
	7.1.1	Investigación de antecedentes	SI	
	7.1.2	Términos y condiciones de contratación.	SI	
	7.2	**Durante la contratación**		
	7.2.1	Responsabilidades de gestión.	SI	
	7.2.2	Concienciación, educación y capacitación en segur. de la información	SI	
	7.2.3	Proceso disciplinario.	SI	
	7.3	**Cese o cambio de puesto de trabajo**		
	7.3.1	Cese o cambio de puesto de trabajo	SI	

GESTIÓN DE ACTIVOS	**8.1**	**Responsabilidad sobre los activos**		
	8.1.1	Inventario de activos.	SI	
	8.1.2	Propiedad de los activos	SI	
	8.1.3	Uso aceptable de los activos.	SI	
	8.1.4	Devolución de activos.	SI	
	8.2	**Clasificación de la información**		
	8.2.1	Directrices de clasificación	SI	
	8.2.2	Etiquetado y manipulado de la información.	SI	
	8.2.3	Manipulación de activos.	SI	
	8.3	**Manejo de los soportes de almacenamiento.**		
	8.3.1	Gestión de soportes extraíbles	SI	
	8.3.2	Eliminación de soportes.	SI	
	8.3.3	Soportes físicos en tránsito.	SI	
CONTROL DE ACCESOS	**9.1**	**Requisitos de negocio para el control de accesos**		
	9.1.1	Política de control de accesos.	SI	
	9.1.2	Control de acceso a las redes y servicios asociados	SI	
	9.2	**Gestión de acceso de usuario**		
	9.2.1	Gestión de altas/bajas en el registro de usuarios.	SI	
	9.2.2	Gestión de los derechos de acceso asignados a usuarios.	SI	
	9.2.3	Gestión de los derechos de acceso con privilegios especiales.	SI	
	9.2.4	Gestión de información confidencial de autenticación de usuarios.	SI	
	9.2.5	Revisión de los derechos de acceso de los usuarios.	SI	
	9.2.6	Retirada o adaptación de los derechos de acceso	SI	
	9.3	**Responsabilidades del usuario.**		
	9.3.1	Uso de información confidencial para la autenticación.	SI	

	9.4	Control de acceso a sistemas y aplicaciones.		
	9.4.1	Restricción del acceso a la información.	SI	
	9.4.2	Procedimientos seguros de inicio de sesión.	SI	
	9.4.3	Gestión de contraseñas de usuario.	SI	
	9.4.4	Uso de herramientas de administración de sistemas.	SI	
	9.4.5	Control de acceso al código fuente de los programas.	SI	
CIFRADO	**10.1**	**Controles criptográficos**		
	10.1.1	Política de uso de los controles criptográficos	SI	
	10.1.2	Gestión de claves	SI	
SEGURIDAD FÍSICA Y AMBIENTAL.	**11.1**	**Áreas seguras**		
	11.1.1	Perímetro de seguridad física.	SI	
	11.1.2	Controles físicos de entrada.	SI	
	11.1.3	Seguridad de oficinas, despachos y recursos.	SI	
	11.1.4	Protección contra las amenazas externas y ambientales.	SI	
	11.1.5	El trabajo en áreas seguras.	SI	
	11.1.6	Áreas de acceso público, carga y descarga.	SI	
	11.2	**Seguridad de los equipos.**		
	11.2.1	Emplazamiento y protección de equipos.	SI	
	11.2.2	Instalaciones de suministro.	SI	
	11.2.3	Seguridad del cableado.	SI	
	11.2.4	Mantenimiento de los equipos.	SI	
	11.2.5	Salida de activos fuera de las dependencias de la empresa.	SI	
	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	SI	
	11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	SI	

	11.2.8	Equipo informático de usuario desatendido.	SI	
	11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	SI	
SEGURIDAD EN LA OPERATIVA	**12.1**	**Responsabilidades y procedimientos de operación**		
	12.1.1	Documentación de procedimientos de operación.	SI	
	12.1.2	Gestión de cambios.	NO	Estas organizaciones por su tamaño, generalmente no poseen sistemas de procesamiento de información.
	12.1.3	Gestión de capacidades.	NO	Estas organizaciones por su tamaño, generalmente cuentan con recursos limitados y por tanto no requiere de proyecciones.
	12.1.4	Separación de entornos de desarrollo, prueba y producción.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	12.2	**Protección contra código malicioso.**		
	12.2.1	Controles contra el código malicioso.	SI	
	12.3	**Copias de seguridad.**		
	12.3.1	Copias de seguridad de la información	SI	
	12.4	**Registro de actividad y supervisión**		
	12.4.1	Registro y gestión de eventos de actividad.	NO	Estas organizaciones no cuentan con sistemas que requieran administrador.
	12.4.2	Protección de los registros de información.	NO	Estas organizaciones no cuentan con sistemas que requieran administrador.
	12.4.3	Registros de actividad del administrador y operador del sistema.	NO	Estas organizaciones no cuentan con sistemas que requieran administrador.
	12.4.4	Sincronización de relojes.	NO	Estas organizaciones por su tamaño, generalmente no poseen sistemas de procesamiento de información.
	12.5	**Control del software en explotación**		

	12.5.1	Instalación del software en sistemas en producción	SI	
	12.6	Gestión de la vulnerabilidad técnica		
	12.6.1	Gestión de las vulnerabilidades técnicas.	SI	
	12.6.2	Restricciones en la instalación de software.	SI	
	12.7	Consideraciones de las auditorías de los sistemas de información		
	12.7.1	Controles de auditoría de los sistemas de información	SI	
SEGURIDAD EN LAS TELECOMUNICACIONES	**13.1**	**Gestión de la seguridad en las redes**		
	13.1.1	Controles de red	SI	
	13.1.2	Mecanismos de seguridad asociados a servicios en red	SI	
	13.1.3	Segregación de redes	SI	
	13.2	**Protección contra código malicioso.**		
	13.2.1	Políticas y procedimientos de intercambio de información	SI	
	13.2.2	Acuerdos de intercambio.	SI	
	13.2.3	Mensajería electrónica.	SI	
	13.2.4	Acuerdos de confidencialidad y secreto	SI	
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	**14.1**	**Requisitos de seguridad de los sistemas de información.**		
	14.1.1	Análisis y especificación de los requisitos de seguridad.	SI	
	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	NO	Estas entidades no tienen conexiones con redes públicas.
	14.1.3	Protección de las transacciones por redes telemáticas.	NO	Estas entidades no realizan transacciones por redes.
	14.2	**Seguridad en los procesos de desarrollo y soporte.**		
	14.2.1	Política de desarrollo seguro de software.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.

	14.2.2	Procedimientos de control de cambios en los sistemas.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.4	Restricciones a los cambios en los paquetes de software.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.5	Uso de principios de ingeniería en protección de sistemas.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.6	Seguridad en entornos de desarrollo.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.7	Externalización del desarrollo de software.	SI	
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.2.9	Pruebas de aceptación.	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
	14.3	**Datos de prueba**		
	14.3.1	Protección de los datos utilizados en pruebas	NO	Estas organizaciones por su tamaño, generalmente no realizan desarrollo de software interno.
RELACIONES CON PROVEEDORES	**15.1**	**Seguridad de la información en las relaciones con suministradores.**		
	15.1.1	Política de seguridad de la información para suministradores.	SI	

	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	SI	
	15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	SI	
	15.2	Gestión de la prestación del servicio por suministradores		
	15.2.1	Supervisión y revisión de los servicios prestados por terceros	SI	
	15.2.2	Gestión de cambios en los servicios prestados por terceros	SI	
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**16.1**	**Gestión de incidentes de seguridad de la información y mejoras.**		
	16.1.1	Responsabilidades y procedimientos.	SI	
	16.1.2	Notificación de los eventos de seguridad	SI	
	16.1.3	Notificación de puntos débiles de la seguridad.	SI	
	16.1.4	Valoración de eventos de seguridad de la información y decisiones	SI	
	16.1.5	Respuesta a los incidentes de seguridad.	SI	
	16.1.6	Aprendizaje de los incidentes de seguridad	SI	
	16.1.7	Recopilación de evidencias	SI	
ASPECTOS DE SEGURIDAD EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**17.1**	**Continuidad de la seguridad de la información**		
	17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	
	17.1.2	Implantación de la continuidad de la seguridad de la información.	SI	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	
	17.2	Redundancias		
	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	SI	

CUMPLIMIENTO	**18.1**	**Cumplimiento de los requisitos legales y contractuales.**		
	18.1.1	Identificación de la legislación aplicable.	SI	
	18.1.2	Derechos de propiedad intelectual (DPI).	SI	
	18.1.3	Protección de los registros de la organización.	SI	
	18.1.4	Protección de datos y privacidad de la información personal.	SI	
	18.1.5	Regulación de los controles criptográficos.	SI	
	18.2	**Revisiones de la seguridad de la información**		
	18.2.1	Revisión independiente de la seguridad de la información.	SI	
	18.2.2	Cumplimiento de las políticas y normas de seguridad.	SI	
	18.2.3	Comprobación del cumplimiento.	SI	

Tabla 1. Evaluación de aplicabilidad

CRITERIOS DE EVALUACIÓN: para realizar el diagnóstico del nivel de madurez en mipymes de asesoría y representación legal, se diseñó una plantilla de evaluación basada en los dominios y objetivos de control de la ISO 27002 de 2013. En dicha plantilla se evalúan tres aspectos principales:

I. Existencia del control.
II. Nivel de formalización e implementación
III. Seguimiento y monitoreo del control

En la tabla No. 2 se definen los aspectos y la definición de cada uno de los campos que pueden ser diligenciados en la plantilla de evaluación.

Campo	Descripción	Descripción de las opciones del campo		
Existencia del control	Describir si el control existe, o no existe	SI	NO	
Cual	En caso de que el control exista se debe hacer una breve descripción del mismo indicando frecuencia, tipo de control y responsable			
Nivel de formalización e implementación	Se debe describir si el control esta formalizado, divulgado y si tiene un responsable	Esta implementado pero no documentado formalmente	Esta implementado y documentado pero no divulgado	Esta implementado, documentado y divulgado
Seguimiento y monitoreo del control	Se debe indicar si existen indicadores y si se realiza monitoreo para el ejecución del control	No hay mecanismos de medición	No se tienen indicadores pero se realiza monitoreo	Se tienen indicadores y se realiza monitoreo

Tabla 2. Criterios de evaluación.

DEFINICIÓN DE PUNTAJES

Por cada objetivo de control se establece un puntaje que permite definir el promedio por dominio. De acuerdo con lo anterior, para establecer el nivel de madurez se definieron los puntajes de la siguiente manera:

Nivel de formalización e implementación:

ITEM	PUNTAJE
Esta implementado pero no documentado formalmente	1
Esta implementado y documentado pero no divulgado	2
Esta implementado, documentado y divulgado	3

Seguimiento y monitoreo del control:

ITEM	PUNTAJE
No hay mecanismos de medición	0
No se tienen indicadores pero se realiza monitoreo	1
Se tienen indicadores y se realiza monitoreo	2

Tabla 3. Puntaje de Implementación/ monitoreo del control.

La suma del nivel de formalización e implementación y el nivel del seguimiento y monitoreo del control, permiten generar el puntaje por objetivo de control que servirá para promediar el puntaje por dominio.

EVALUACIÓN Y RESULTADOS

Para la evaluación de cada dominio, se tomó como referencia los atributos que deben cumplir los controles basados en Cobit 4.1 [6] ajustados de acuerdo al criterio de los autores:

Escala	Características
0	***No Existe***: La empresa no ha reconocido siquiera que existe un problema a resolver.
1	***Inicial:*** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar. El enfoque general hacia la administración es desorganizado.
2	***Repetible***: Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo.
3	***Definido:*** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4	***Administrado:*** Es posible monitorear pero no medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora.
5	***Optimizado:*** Los procesos se basan en los resultados de mejoras continuas. Se monitorea y se mide el cumplimiento de los objetivos, La seguridad se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Tabla 4. Escala de evaluación (Tomado de Cobit 4.1)

12. METODOLOGÍA PARA IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Los activos de información en todas las entidades son muy importantes y por tanto requieren protección adecuada. Por ello, se hace necesario tener una metodología que permita identificarlos y clasificarlos por su confidencialidad, integridad y disponibilidad. Esto permitirá que las entidades tengan un inventario de activos de información debidamente clasificado.

Con la metodología que se plantea se busca que los Gerentes o Responsables de las Mipymes de Asesoría y representación legal, identifiquen cuál de la información que manejan en dichas entidades es sensible, con el fin que se tomen las medidas pertinentes para su respectivo manejo, acceso y control. Esta metodología es aplicable a toda la información magnética y física, que fluye por la ejecución de las actividades propias del proceso, involucrando toda aquella información que procede de otras áreas o entes externos.

La metodología planteada se basa en MAGERIT, la cual ha sido adaptada y ajustada por los autores de acuerdo a su experiencia académica y profesional, para su aplicación en Mipymes de asesoría y representación legal

TIPOLOGIAS DE LOS ACTIVOS INFORMACION

Para poder efectuar el análisis y la clasificación de los activos en los siguientes numerales, se hace necesario partir de una tipología que permita identificar todos los componentes relacionados con un activo de información. Dichas tipologías son las siguientes:

Componentes de SI en una organización	Tipologías	Descripción
Tipos de almacenamiento de activos de información	Magnético (Digital)	Cualquier tipo de información contenida en un medio digital, bien sea en forma de bases de datos, archivos de datos, o cualquier información archivada electrónicamente. (Ej. Evidencias, BD de clientes, etc.)
	Documento / Registro (Físico)	Cualquier tipo de información que se encuentre en medio impreso. (Ej., Expedientes, citaciones, etc.).
Ubicación y Contenedores de activos de información	Hardware	Cualquier componente de hardware que sea necesario para efectuar o complementar operaciones sobre algún activo de información.
	Dispositivos de almacenamiento Digital	Cualquier tecnología de almacenamiento extraíble que sea necesaria para efectuar o complementar alguna operación sobre otros activos de información; por ejemplo: USB, CDs, DVDs, discos externos, entre otros.
	Infraestructura Física	Aquellas instalaciones o estructuras diseñadas y construidas para cumplir una actividad específica, que permitan ofrecer un servicio requerido por la entidad y alojar los activos de información.

Custodios y responsables	Persona	Funcionario o ente externo que realice funciones críticas para la entidad, cuya ausencia o incumplimiento de tales funciones puede desencadenar un impacto para el mismo.
Aplicaciones o herramientas de procesamiento	Software	Todo sistema de información o software adquirido que utilice activos de información para efectuar sus tareas.

Tabla 5. Tipologías activos de Seguridad de la Información

De acuerdo a lo anterior, se puede comprender que los activos en una empresa pueden ser clasificados en una de las anteriores tipologías, de tal manera que se puede continuar con el análisis detallado en la plantilla de identificación de activos de información que se presenta a continuación,

PLANTILLA DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Considerando las tipologías de activos de Seguridad de la Información, se diseñó una plantilla que permite identificar de forma fácil y estructurada los activos de información. Para la aplicación de esta plantilla de identificación de activos de información, en primer lugar es necesario diligenciar la plantilla con las siguientes indicaciones:

a) **ETAPA I**: Identificación e inventario de los activos de información

En esta etapa se pretende identificar los activos de información por actividad realizada por la entidad, dando un nombre al activo, su descripción y justificación. De igual forma se le puede asignar un código para poder identificarlo, cuya nemotecnia dependerá de la entidad.

Código	Nombre del activo	Descripción	Justificación

Estos datos deben ser diligenciados por el dueño del proceso, o por un delegado que conozca claramente cada uno de ellos y pueda identificarlos. Esta etapa es primordial ya que este es el inventario inicial de los activos de información. Los activos que se diligenciarán en esta etapa son los correspondientes a los tipos: "Magnético" y "Documento" vistos en el ítem anterior.

b) **ETAPA II**: Características básicas de los activos de información

En esta etapa se diligenciarán las características más importantes de los activos de información como lo son:

- APLICACIÓN: indicar si se genera de alguna aplicación de software que tenga la entidad.

- TIPOS DE ALMACENAMIENTO: se debe especificar si el activo de información de tipo documento, Magnético, o está almacenado en ambos formatos.

- CONTENEDOR: indicar en éste campo el repositorio físico o digital donde reside o se almacena el activo de información durante el proceso. Aquí se debe tener en cuenta los tipos de activos de información (ejemplo de contenedores físicos: archivador, gaveta, etc.) (ejemplo de contenedores digitales: hardware, dispositivos de almacenamiento digital, etc.)

- UBICACIÓN: en este campo se debe diligencia el sitio físico donde se encuentra el contenedor, teniendo en cuenta la tipología: infraestructura física (ejemplo: oficinas, edificios, etc.).

- CUSTODIOS Y/O RESPONSABLES: en este campo se deben diligenciar todas las personas que custodian el activo de información y/o aquellos que son responsables del activo.

Aplicación	Tipos de almacenamiento	Contenedor	Ubicación	Custodio / responsable

c) **ETAPA III:** Clasificación de Activos de Información

Esta etapa es una de las más importantes y requiere que el responsable o dueño de la información realice la clasificación, ya que medirá el nivel de impacto de cada activo para poder clasificarlo por confidencialidad, integridad y disponibilidad.

Debido a la baja complejidad de las Mipymes de asesoría y representación legal en los aspectos de manejo y procesamiento de información, se ha decidido diseñar una escala de solo tres niveles, lo que la hace más práctica y más fácil de aplicar, pero sin afectar el nivel de análisis efectuado.

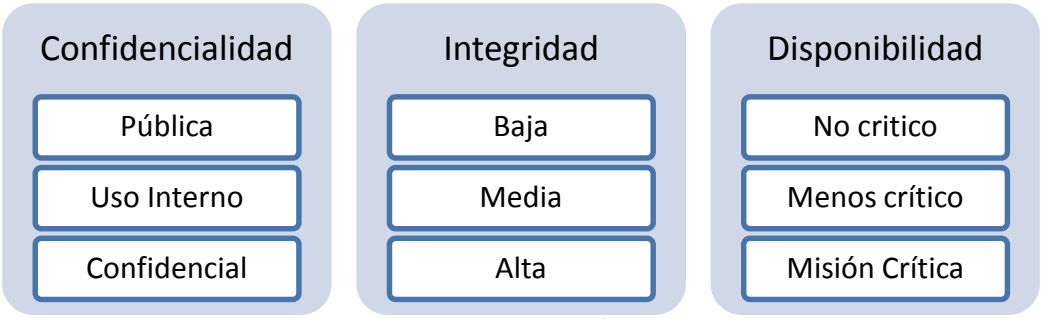


Figura 4 Clasificación de activos

A partir de la respuesta a las siguientes preguntas se puede determinar el nivel de sensibilidad de la información.

- **CONFIDENCIALIDAD**: Si la respuesta es “SI” a alguno de los ítem según su categoría se determina su nivel de confidencialidad.

Público	Es información aprobada para presentarse fuera de la entidad a través de comunicados externos o fines publicitarios
	Esta información está actualmente a disposición del público
	Es información de mercadeo actualmente distribuida al público
	Es información que puede divulgarse al público y que no beneficia a los competidores, no impacta negativamente a la entidad y no genera brechas de privacidad.
	Esta información está disponible al público a través de comunicados de prensa u otros medios masivos de comunicación.
	Son datos personales públicos, calificados como tal según los mandatos de la ley o de la constitución política (son públicos, entre otros, los datos contenidos en documentos públicos y los relativos al estado civil de las personas)
Uso interno	Es información relacionada con políticas, estándares, procedimientos, comunicados internos, organigramas o directorios telefónicos internos
	Es información que se puede distribuir en boletines, folletos o memorandos internos o publicar en sitios internos.
	Es información que se puede divulgar sin restricción a todos los funcionarios y que puede divulgarse a externos con aprobación
	Son datos personales que no tienen naturaleza íntima, reservada o privada y cuyo conocimiento o divulgación puede interesar a todos los funcionarios de la entidad
Confidencial	Es Información que se debe mantener en secreto o guardar reserva y discreción, sean datos de clientes o relacionados con la situación propia de la entidad
	Es información sensible o secreta que si se divulga o usa sin autorización puede generar un serio impacto (por ejemplo, en las relaciones con clientes o en su imagen pública)
	Es información relacionada con datos personales de los funcionarios
	Es información amparada por los derechos constitucionales a la intimidad o fundamentada en el principio del secreto profesional
	Son informes, reportes o investigaciones de: fraudes, ilícitos, mala conducta, violación de leyes o políticas, procesos disciplinarios o incidentes de seguridad
	La información incluye datos específicos de protocolos de seguridad, como: llaves de cifrado, contraseñas o firmas digitales
	Son datos personales privados que por su naturaleza íntima o reservada sólo es relevante para su titular
	Es información de circulación restringida que se deriva de la naturaleza de los datos y de las disposiciones legales

Tabla 6. Ítems Confidencialidad

INTEGRIDAD: Si la respuesta es “SI” a alguno de los ítem según su categoría se determina su nivel de Integridad.

Bajo	La pérdida o modificación no autorizada de esta información no causa daños a la organización.
	La pérdida o modificación no autorizada de esta información No genera sanciones o pérdidas económicas para la Organización.
	La pérdida o modificación no autorizada de esta información no causaría una pérdida de imagen o reputación significativa para la Organización.
	La pérdida o modificación no autorizada de esta información no hacer que existan reclamaciones por parte de los clientes y/o funcionarios.
	La pérdida o modificación no autorizada de esta información No afecta la oportunidad de la información.
Medio	La pérdida o modificación no autorizada de esta información Puede generar sanciones o pérdidas económicas para la Organización, siendo éstas recuperables y/o no muy significativas.
	La pérdida o modificación no autorizada de esta información Puede causar una leve o moderada pérdida de imagen o reputación de la Organización.
	La pérdida o modificación no autorizada de esta información Podrían existir reclamaciones por parte de los clientes y/o proveedores pero no se afecta la continuidad de la relación.
	La pérdida o modificación no autorizada de esta información Pueden generarse inconvenientes o perjuicios legales.
	La pérdida o modificación no autorizada de esta información Pérdida de información crítica de la Organización o de terceros que no se pueda recuperar fácilmente.
	La pérdida o modificación no autorizada de esta información Puede generar reproceso de actividades y aumento de la carga operativa.
Alto	La pérdida o modificación no autorizada de esta información Podría causar daños económicos materiales para la Organización.
	La pérdida o modificación no autorizada de esta información Puede generar un impacto importante en la imagen o reputación de la Organización.
	La pérdida o modificación no autorizada de esta información Pueden generarse sanciones económicas para la Organización, por parte de autoridades legales.
	La pérdida o modificación no autorizada de esta información puede hacer que existan reclamaciones por parte de clientes y/o proveedores.
	La pérdida o modificación no autorizada de esta información Puede generar inconvenientes o perjuicios legales.
	La pérdida o modificación no autorizada de esta información hace que exista pérdida de información crítica de la Organización o de terceros que no se pueda recuperar.

Tabla 7. Ítems Integridad

DISPONIBILIDAD: Si la respuesta es “SI” a alguno de los ítem según su categoría se determina su nivel de Disponibilidad.

No crítico	La información puede no estar disponible por un período de tiempo extendido y por tanto no genera sanciones o pérdidas económicas significativas para la Organización.
	La información puede no estar disponible por un período de tiempo extendido y por tanto no causaría una pérdida de imagen o reputación significativa para la Organización.
	La información puede no estar disponible por un período de tiempo extendido y por tanto no hay reclamaciones por parte de los clientes
	La información puede no estar disponible por un período de tiempo extendido y por tanto puede afectar levemente la oportunidad de la información.
Menos Crítico	La información puede no estar disponible por un período de tiempo extendido y por tanto Puede generar sanciones o pérdidas económicas para la Organización, siendo éstas recuperables y/o no muy significativas.
	La información puede no estar disponible por un período de tiempo extendido y por tanto puede causar una leve o moderada pérdida de imagen o reputación de la Organización.
	La información puede no estar disponible por un período de tiempo extendido y por tanto podrían existir reclamaciones por parte de los clientes pero no se afecta la continuidad de la relación.
	La información puede no estar disponible por un período de tiempo extendido y por tanto podrían generarse inconvenientes o perjuicios legales.
	La información puede no estar disponible por un período de tiempo extendido y por tanto podrían generarse reproceso de actividades y aumento de la carga operativa.
	La información puede no estar disponible por un período de tiempo extendido y por tanto puede afectar de manera importante la oportunidad de la información.
Misión Crítica	La información puede no estar disponible por un período de tiempo extendido y por tanto podría causar daños económicos materiales.
	La información puede no estar disponible por un período de tiempo extendido y por tanto puede generar un impacto importante en la imagen o reputación de la Organización.
	La información puede no estar disponible por un período de tiempo extendido y por tanto pueden generarse sanciones económicas para la Organización, por parte de autoridades legales o entes reguladores.
	La información puede no estar disponible por un período de tiempo extendido y por tanto hay reclamaciones por parte de clientes.
	La información puede no estar disponible por un período de tiempo extendido y por tanto pueden generarse inconvenientes o perjuicios legales.
	La información puede no estar disponible por un período de tiempo extendido y por tanto puede afectar de manera significativa la oportunidad de la información.

Tabla 8. Ítems Disponibilidad

d) **ETAPA IV:** Identificación de Contenedores Críticos

Considerando la clasificación de activos realizado en las etapas anteriores, se deben seleccionar los contenedores que contienen activo de información críticos para la entidad.
Para esto es necesario validar si el activo de información cumple con las siguientes condiciones:

Confidencialidad	Integridad	Disponibilidad	Criticidad del contenedor
Confidencial	Alta	Misión Crítica	Alta
Confidencial	Alta	Menos critico	Alta
Confidencial	Alta	No critico	Alta
Confidencial	Media	Misión Crítica	Alta
Confidencial	Media	Menos critico	Media
Confidencial	Media	No critico	Media
Confidencial	Bajo	Misión Crítica	Alta
Confidencial	Bajo	Menos critico	Media
Confidencial	Bajo	No critico	Media
Uso interno	Alta	Misión Crítica	Alto
Uso interno	Alta	Menos critico	Alto
Uso interno	Alta	No critico	Media
Uso interno	Media	Misión Crítica	Media
Uso interno	Media	Menos critico	Media
Uso interno	Media	No critico	Media
Uso interno	Bajo	Misión Crítica	Media
Uso interno	Bajo	Menos critico	Media
Uso interno	Bajo	No critico	Media
Público	Alta	Misión Crítica	Alto
Público	Alta	Menos critico	Medio
Público	Alta	No critico	Medio
Público	Media	Misión Crítica	Medio
Público	Media	Menos critico	Bajo
Público	Media	No critico	Bajo
Público	Bajo	Misión Crítica	Medio
Público	Bajo	Menos critico	Bajo
Público	Bajo	No critico	Bajo

Tabla 9. Criterios de clasificación de contendores

En esta etapa se les da prioridad a los contenedores críticos y a estos se les realizará el análisis y evaluación de riesgos.

A continuación se presenta un diagrama explicativo de las etapas de la metodología de identificación de activos de información mencionadas anteriormente.

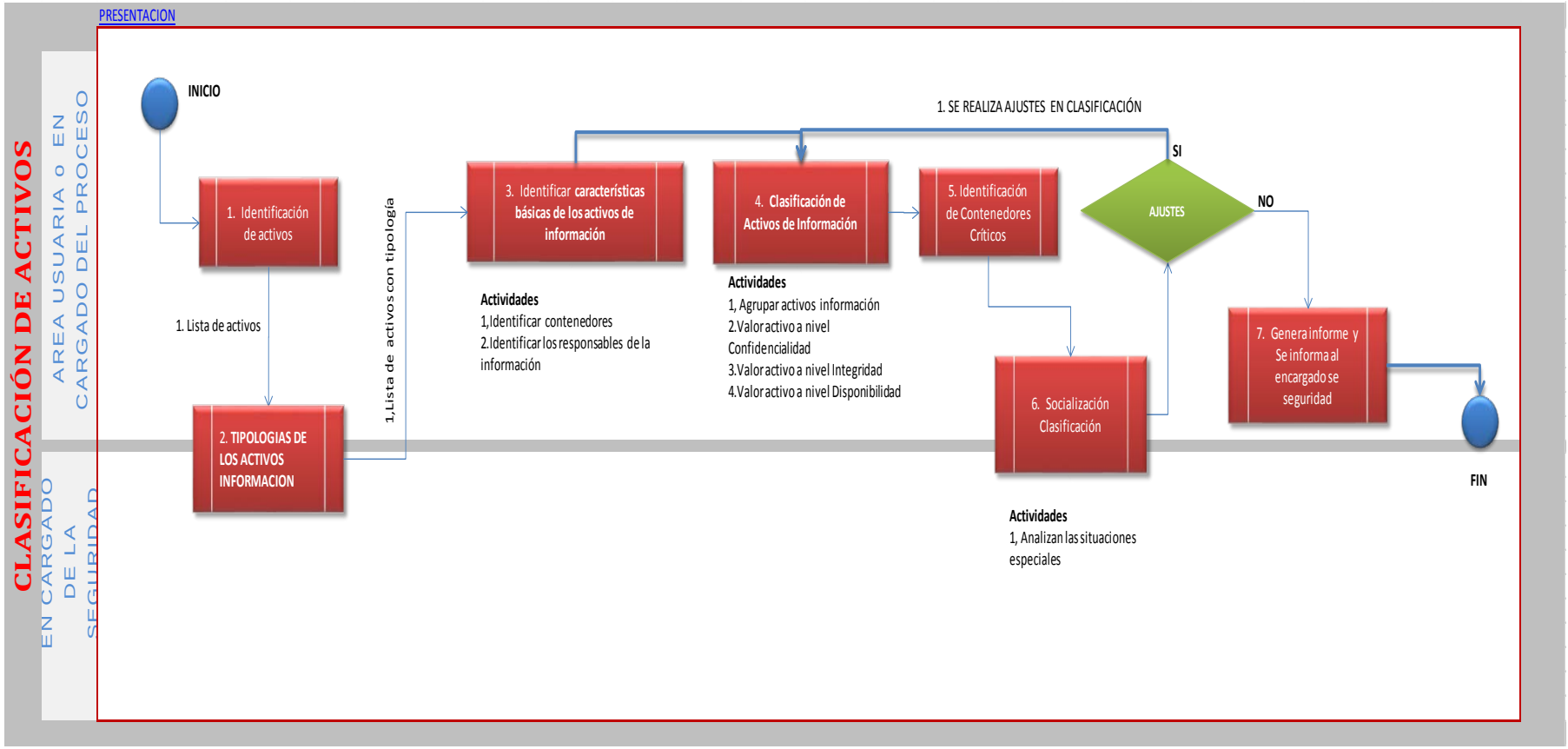


Figura 5 Proceso de clasificación activos

13. METODOLOGÍA PARA ANALISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD

Teniendo en cuenta los contenedores identificados en la etapa anterior, el siguiente paso consiste en realizar un análisis y evaluación de riesgos asociados a los mismos.

a. **ETAPA I:** Identificación de amenazas y vulnerabilidades

Identificación de amenazas: identificación de actividades, eventos o acciones que impliquen daños a los activos de información definidos. A continuación se presenta una recopilación realizada por los autores de las amenazas más comunes que podrían afectar a las Mipymes de asesoría y representación legal:

- Acceso físico no autorizado
- Ausencia / Interrupción en el suministro eléctrico o de telecomunicaciones
- Funcionamiento inadecuado de la infraestructura de TI
- Instalación o implantación de código malicioso
- Accidente importante que afecta la instalación
- Situaciones de Contaminación ambiental
- Degradación de los medios en lo que se almacena información
- Fenómeno sísmico
- Incendio
- Inundación
- Actos malintencionados
- Corrupción de la información
- Acceso no autorizado a la información

Identificación de vulnerabilidades: identificación de condiciones o características que podrían hacer a los activos de información susceptibles a amenazas. A continuación se presenta una recopilación realizada por los autores de las vulnerabilidades más comunes:

- Construcción deficiente de edificios
- Acceso no supervisado a las oficinas/edificios/instalaciones
- Ausencia de mecanismos de control de acceso físico a las instalaciones
- Ausencia de personal de seguridad física (vigilancia)
- Falta de mecanismos de protección física de las instalaciones físicas
- Falta de mecanismos de monitoreo (ej. Cámaras de vigilancia, detectores de humedad, detectores de humo, etc.)
- Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas
- Falta de elementos de soporte (UPS)
- Fluctuaciones Eléctricas
- Los equipos no reciben mantenimiento preventivo adecuado y suficiente (ej. componentes de TI, sistemas contra incendios, de suministro de energía, etc.)

- Falta de la copia de respaldo (backup)
- Inexistencia de planes de continuidad de negocio
- Ausencia de supervisión sobre los trabajos realizados por personal externo
- Ausencia de control en la descarga y uso de software
- Software antivirus desactualizado
- No aplicación de parches de seguridad liberados por los proveedores de soluciones de TI
- Uso de código no autorizado o no probado
- Ausencia de señalización adecuada al interior de las instalaciones.
- Inexistencia de planes de continuidad de negocio
- Ubicación de las instalaciones en sector de alto riesgo (inundación, terremoto, etc.)
- Falta de personal de limpieza
- Falta de políticas de escritorio y pantalla limpia
- Copias de respaldo en mal estado
- Materiales inflamables empleados en la construcción y acabado de las instalaciones
- Materiales inflamables en inmediaciones
- Sistemas insuficientes contra incendios
- Acceso no restringido a los recursos de información
- Administración indebida de cuentas y contraseñas de acceso
- Almacenamiento de contraseñas de acceso en texto claro
- Copias de respaldo desprotegidas
- Asignación errada de privilegios de acceso a los usuarios
- Recursos de tecnología de información que no cuentan con esquemas de autenticación de usuarios (cuentas y contraseñas de acceso)
- Ausencia de perfiles de acceso de los usuarios
- Realización no autorizada de copias de respaldo y/o restauración de la mismas
- Inadecuada definición y/o ausencia de cláusulas de seguridad de la información en los contratos con empleados, clientes y terceras partes
- Existencia de cuentas y contraseñas de acceso genéricas
- Existencia de cuentas de acceso activas asignadas a personal retirado.
- Inadecuada segregación de funciones en los perfiles de acceso sobre los sistemas de información
- Información de valor para el negocio desprotegida en los puestos de trabajo
- Cuentas y contraseñas de acceso que se comparten entre varios funcionarios
- Pérdida de los equipos de trabajo y/o sus dispositivos
- Puertos o servicios inseguros habilitados (ftp, telnet, etc.)
- Ubicación susceptible a disturbios, robos o vandalismo.
- Uso no controlado del correo electrónico.
- Acceso de personal no autorizado a la información almacenada en copias de respaldo
- Definición de contraseñas de acceso triviales
- Modificación no autorizado de información
- Ausencia de mecanismos de control de acceso lógico desde internet a los recursos de información de la Firma (firewalls, etc.).
- Ausencia de un programa de concienciación de seguridad de la información

- Ausencia de una estructura organizacional responsable por ejecutar la función de seguridad de la información
- Brechas en las obligaciones definidas en los contratos
- Destrucción no autorizado de información
- Existencia de cuentas de acceso por defecto en los recursos de TI
- Falta de concientización en seguridad
- No existen procedimientos que garanticen la devolución de los activos o bienes de información al finalizar la relación laboral o contractual
- Ausencia de acuerdos de confidencialidad firmados
- Uso no restringido de dispositivos de almacenamiento extraíbles
- No se verifican de manera periódica las cuentas de acceso y los privilegios asignados

ETAPA II: Definición de amenazas por vulnerabilidad

En la tabla se realiza un listado de amenazas y su posible vulnerabilidad para la identificación de los riesgos asociados según corresponda, por contenedor:

Amenaza	Vulnerabilidad
Acceso físico no autorizado	Construcción deficiente de edificios
	Acceso no supervisado a las oficinas/edificios/instalaciones
	Ausencia de mecanismos de control de acceso físico a las instalaciones
	Ausencia de personal de seguridad física (vigilancia)
	Falta de mecanismos de protección física de las instalaciones físicas
	Falta de mecanismos de monitoreo (ej. Cámaras de vigilancia, detectores de humedad, detectores de humo, etc.)
	Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas
Ausencia / Interrupción total o parcial en el suministro eléctrico	Falta de elementos de soporte (UPS)
	Fluctuaciones Eléctricas
	Los equipos no reciben mantenimiento preventivo adecuado y suficiente (ej. componentes de TI, sistemas contra incendios, de suministro de energía, etc.)
Funcionamiento inadecuado de la infraestructura de TI	Los equipos no reciben mantenimiento preventivo adecuado y suficiente (ej. componentes de TI, sistemas contra incendios, de suministro de energía, etc.)
	Falta de copias de respaldo (backup)
	Inexistencia de planes de continuidad de negocio
	Ausencia de supervisión sobre los trabajos realizados por personal externo
Instalación o implantación de código malicioso	Ausencia de control en la descarga y uso de software
	Software antivirus desactualizado
	No aplicación de parches de seguridad liberados por los proveedores de soluciones de TI
	Uso de código no autorizado o no probado
Accidente importante que afecta la instalación	Ausencia de señalización adecuada al interior de las instalaciones.
	Construcción deficiente de edificios
	Falta de mecanismos de monitoreo (ej. Cámaras de vigilancia, detectores de humedad, detectores de humo, etc.)
	Falta de supervisión de mecanismos de monitoreo
	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información
	Inexistencia de planes de continuidad de negocio

	Ubicación de las instalaciones en sector de alto riesgo (inundación, terremoto, etc.)
Situaciones de Contaminación ambiental (polvo, etc.)	Falta de personal de limpieza
	Falta de políticas de escritorio y pantalla limpia
Degradación de los medios en lo que se almacena información	Falta de personal de limpieza
	Falta de copias de respaldo (backup)
	Copias de respaldo en mal estado
Fenómeno sísmico	Construcción deficiente de edificios
	Ubicación de las instalaciones en sector de alto riesgo (inundación, terremoto, etc.)
	Inexistencia de planes de continuidad de negocio
Incendio	Construcción deficiente de edificios
	Falta de mecanismos de monitoreo (ej. Cámaras de vigilancia, detectores de humedad, detectores de humo, etc.)
	Falta de supervisión de mecanismos de monitoreo
	Los equipos no reciben mantenimiento preventivo adecuado y suficiente (ej. componentes de TI, sistemas contra incendios, de suministro de energía, etc.)
	Materiales inflamables empleados en la construcción y acabado de las instalaciones
	Sistemas insuficientes contra incendios
	Inexistencia de planes de continuidad de negocio
Inundación (sabotaje en tuberías, etc.)	Construcción deficiente de edificios
	Falta de mecanismos de monitoreo (ej. Cámaras de vigilancia, detectores de humedad, detectores de humo, etc.)
	Falta de supervisión de mecanismos de monitoreo
	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información
	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)
	Inexistencia de planes de continuidad de negocio
Actos malintencionados (vandalismo, etc.)	Acceso no restringido a los recursos de información
	Administración indebida de cuentas y contraseñas de acceso
	Almacenamiento de contraseñas de acceso en texto claro
	Copias de respaldo desprotegidas
	Asignación errada de privilegios de acceso a los usuarios
	Recursos de tecnología de información que no cuentan con esquemas de autenticación de usuarios (cuentas y contraseñas de acceso)
	Ausencia de perfiles de acceso de los usuarios
	Realización no autorizada de copias de respaldo y/o restauración de la mismas
	Ausencia de control en la descarga y uso de software
	Software antivirus desactualizado
	Inadecuada definición y/o ausencia de cláusulas de seguridad de la información en los contratos con empleados, clientes y terceras partes
	Divulgación de información confidencial
	Existencia de cuentas y contraseñas de acceso genéricas
	Existencia de cuentas de acceso activas asignadas a personal retirado
	Inadecuada segregación de funciones en los perfiles de acceso sobre los sistemas de información
	Información de valor para el negocio desprotegida en los puestos de trabajo
	Cuentas y contraseñas de acceso que se comparten entre varios funcionarios
	Pérdida de los equipos de trabajo y/o sus dispositivos

	Puertos o servicios inseguros habilitados (ftp, telnet, etc.)
	Ubicación susceptible a disturbios, robos o vandalismo.
	Uso no controlado del correo electrónico.
Corrupción de la información	Asignación errada de privilegios de acceso a los usuarios
	Definición de contraseñas de acceso triviales
	Existencia de cuentas de acceso activas asignadas a personal retirado
	Cuentas y contraseñas de acceso que se comparten entre varios funcionarios
	Modificación no autorizado de información
	Puertos o servicios inseguros habilitados (v.gr. ftp, telnet, etc.)
Acceso no autorizado a la información	Definición de contraseñas de acceso triviales
	Existencia de cuentas y contraseñas de acceso genéricas
	Existencia de cuentas de acceso por defecto en los recursos de TI
	Existencia de cuentas de acceso activas asignadas a personal retirado
	Falta de políticas para la conservación y retención de eventos de seguridad
	No se verifican de manera periódica las cuentas de acceso y los privilegios asignados
	Pérdida de los equipos de trabajo y/o sus dispositivos (v.gr. equipos portátiles, USB, Discos Portátiles, etc.)
	Ausencia de acuerdos de confidencialidad firmados
	Falta de concientización en seguridad
	Falta de depuración de usuarios de los sistemas de información
	No existen procedimientos que garanticen la devolución de los activos o bienes de información al finalizar la relación laboral o contractual.
	Uso no controlado del correo electrónico.
	Uso no restringido de dispositivos de almacenamiento extraíbles

Tabla 10. Amenazas y vulnerabilidades

ETAPA III: Escala de Probabilidad

Una vez identificados los riesgos, es necesario determinar la probabilidad de ocurrencia para ello se seleccionaron las siguientes escalas de valoración:

CATEGORÍA	VALOR CATEGORÍA	DESCRIPCIÓN
INMINENTE	**5**	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo y por tanto la materialización de la amenaza ocurre diariamente.
FRECUENTE	**4**	La materialización de la amenaza ocurre una vez a la semana.
OCASIONAL	**3**	La materialización de la amenaza ocurre una vez al mes.
REMOTO	**2**	La materialización de la amenaza ocurre una vez al año.
IMPROBABLE	**1**	La amenaza no posee la suficiente motivación y capacidad o nunca se ha materializado la amenaza pero no se descarta su ocurrencia.

Tabla 11 Escala de probabilidad

ETAPA IV: Escala de impactos

Como siguiente pasó, se debe estimar la severidad de las consecuencias en caso de que se materialice el riesgo, para ello se contemplan las siguientes escalas:

CATEGORÍA	VALOR CATEGORÍA	IMPACTO FINANCIERO	IMPACTO REPUTACIONAL	IMPACTO LEGAL
CATASTRÓFICO	**5**	Las pérdidas estimadas son mayores al 1% del total del valor de los activos de la entidad.	Se afecta gravemente la imagen de la Entidad, hay pérdida de credibilidad y opinión pública negativa. Hay divulgación en medios de comunicación.	Incumplimiento de la normatividad legal vigente establecida en Colombia (Constitución, leyes, decretos).
SEVERO	**4**	Las pérdidas estimadas que oscilan entre 0,5% y 1% del total del valor de los activos de la entidad.	Se afecta la imagen de la Entidad, por pérdida de credibilidad y opinión pública negativa.	Incumplimiento de la normatividad exigida por los entes reguladores y de control.
MODERADO	**3**	Las pérdidas estimadas que oscilan entre 0,3% y 0,5% del total del valor de los activos de la entidad.	Puede generarse una opinión pública negativa sobre la prestación del servicio.	Incumplimiento de las Políticas internas de Seguridad
LEVE	**2**	Las pérdidas estimadas que oscilan entre 0,1% y 0,2% del total del valor de los activos de la entidad.	La afectación de la Imagen de la Entidad es Leve y resolver este tema implica recursos y puede durar buen tiempo.	Incumplimiento a los procedimientos y prácticas definidas para la operación adecuada del Seguridad.
INSIGNIFICANTE	**1**	Las pérdidas estimadas menores a 0,1% del total del valor de los activos de la entidad.	La afectación de la Imagen de la Entidad es insignificante y fácil de resolver.	No genera afectación legal.

Tabla 12. Escalas de Impacto

Para porcentajes de los niveles de impacto financiero definidos en la tabla anterior, se puede tener en cuenta la suma de los activos: circulante, diferido y fijo. Sin embargo, dichos porcentajes deben ser establecidos por la alta Gerencia, la tabla muestra a manera de ejemplo como pueden ser calculados.

Para el impacto legal se fundamentó en los deberes establecidos en los numerales 1º y 11 del artículo 153 de la Ley 270 de 1996 y Ley 1581 de 2012 y al Decreto 1377 de 2013. El propósito principal de la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones.

ETAPA V: Ubicación de los riesgos y análisis

A continuación se presenta el mapa de riesgos propuesto, teniendo en cuenta las escalas de probabilidad e impacto definidas previamente.

- Color verde: Indica riesgos que tienen una valoración baja
- Color amarillo: indican una valoración media.
- Color naranja: indican una valoración alta.
- Color rojo: indican una valoración extrema.

Para la lectura de la matriz se debe tener en cuenta que en la zona roja caerían aquellos riesgos Extremos, o sea de una alta probabilidad de ocurrencia o de consecuencias muy altas. Mientras los de color naranja son de riesgo alto porque su probabilidad es alta y altas también son las consecuencias que se derivan. Por otro lado, los amarillos son de riesgo medio y los verdes de riego bajo.

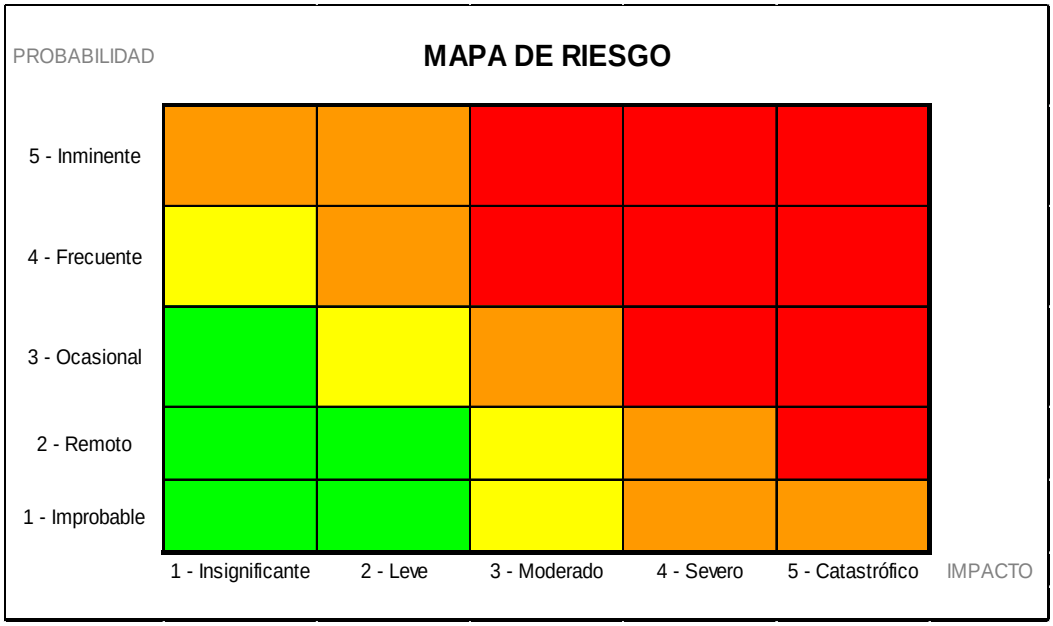


Figura 6 Mapa de riesgos

.

Etapa VI Manejo del Riesgo

Consiste en determinar los controles existentes de los riesgos y causas identificadas, con el fin de determinar qué tan efectivos son en la reducción de la probabilidad y/o el impacto de los riesgos inherentes.

Adicionalmente, en esta etapa se identifican los controles que actualmente se tienen para mitigar los riesgos, con el fin de evaluar su efectividad en la implementación de los controles y la reducción del impacto en caso que el riesgo se materialice.

El resultado final de esta etapa es la generación del mapa de riesgos residual el cual se obtiene de la medición de la efectividad de los controles existentes, que buscan minimizar el grado de severidad y el nivel de riesgo de los riesgos inherentes.

Estrategia de Manejo; Los controles permiten:

- Reducir la probabilidad
- Reducir el impacto
- Transferir el riesgo
- Evitar el riesgo

Tipos de controles

- Preventivo: Reducen la frecuencia con que ocurren las causas del riesgo.
- Detectivo - Correctivos: No evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridas.
- Correctivos: Corrigen las causas del riesgo, este tipo de control permite reducir el impacto en los activos.

Descripción Del Proceso de Análisis De Riesgos

- Programar el análisis/actualización de riesgos

Las actividades de esta fase son:

- ✓ Se define el recurso de información (proceso, activo de la información o contenedor) al que se le realizará el análisis de riesgos o su actualización.
- ✓ Se Informa a las áreas involucradas, a través de correo electrónico sobre el análisis a realizar, con el objetivo que designe el encargado o quien haga sus veces, para desarrollar esta actividad.

- Contextualización de la actividad

Las actividades de esta fase son:

- ✓ Previo a las entrevistas, se recopila y revisa la información relacionada con el proceso, activo de la información o contenedor a analizar, a través de la información relacionada con incidentes de seguridad registrados o que sean informados por los encargados del activo de información.
- ✓ Aclara dudas respecto a la información revisada, en la entrevista de análisis/seguimiento.
- ✓ Como la salida de esta fase se obtendrá la siguiente información:
- ✓ Lista de clasificación de la Información.
- ✓ Lista de riesgos en el caso que existan.

- Analizar cualitativamente el riesgo inherente:

En esta fase se utiliza la metodología de análisis y evaluación de riesgos de seguridad definida en el presente documento, donde se:

- ✓ Identifica las vulnerabilidades, amenazas, se asocian amenazas por vulnerabilidad, riesgos y criterios que afectan la seguridad de los activos de información de acuerdo a la metodología establecida.
- ✓ A juicio de expertos, ambas partes (riesgos y el área analizada) deben valorar la probabilidad y el impacto inherente de cada uno de los riesgos identificados, asumiendo el peor escenario, en donde no haya controles, teniendo como base los registros históricos de incidentes u otras evidencias.
  " pueden participar en esta calificación las áreas usuarias y las áreas de control(En los casos que existan)"

- Tratamiento del riesgo

  En esta fase del proceso se realiza las siguientes actividades:

  - ✓ Se Definen controles, acciones vs riesgo y se establece limite o alcance de los controles, esto se debe realizan en conjunto con el encargado de gestionar la seguridad y el dueño del activo de la información.
  - ✓ Se indican y describen los controles alineados a la norma ISO 27002 existentes que permitan minimizar o mitigar los riesgos identificados en la actividad anterior.
  - ✓ Se califican los controles identificados para cada uno de los riesgos asociados a los contenedores de la información.

  Como la salida de esta fase se obtendrá la siguiente información:

  - ✓ Valoración de riesgo Inherente.
  - ✓ Valoración de riesgo Residual.
  - ✓ Lista de controles.

- **Socialización de los riesgos residual**

En esta fase del proceso se realiza las siguientes actividades:

- ✓ Se socializa los riesgos residuales, producto del resultado de la aplicación de los controles sobre el valor de la probabilidad e impacto inherente de los riesgos identificados en los activos de la información.
- ✓ Se analizan las situaciones especiales que deban ser mitigadas y/o mejoradas.

Si se presentan ajustes se retorna a la fase de tratamiento de los riesgos y se realiza nuevamente la valoración.

- **Actualización de mapas de riesgo**

Esta fase del proceso se realiza las siguientes actividades:

El encargado de la seguridad en conjunto con el dueño del activo de la información realiza la actualización de los mapas de riesgos inherentes y residuales con la relación del código de las amenazas y de los riesgos como se evidencia en la figura.

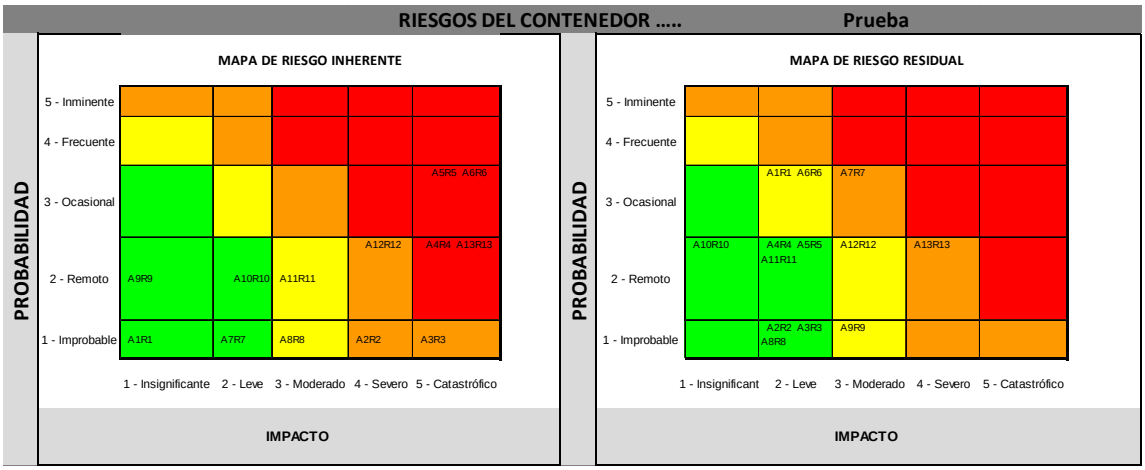


Figura 7 Matrices de riesgo (ejemplo)

- **Genera informe del análisis de riesgo**

En esta fase el encargo de la seguridad realiza un informe con los resultados de la evaluación de los riesgos, controles y las de excepción, los cuales se deben presentar a la gerencia.

Como salida de esta fase se obtiene la siguiente información:

- ✓ “Informe sobre Eval. Riesgos”.

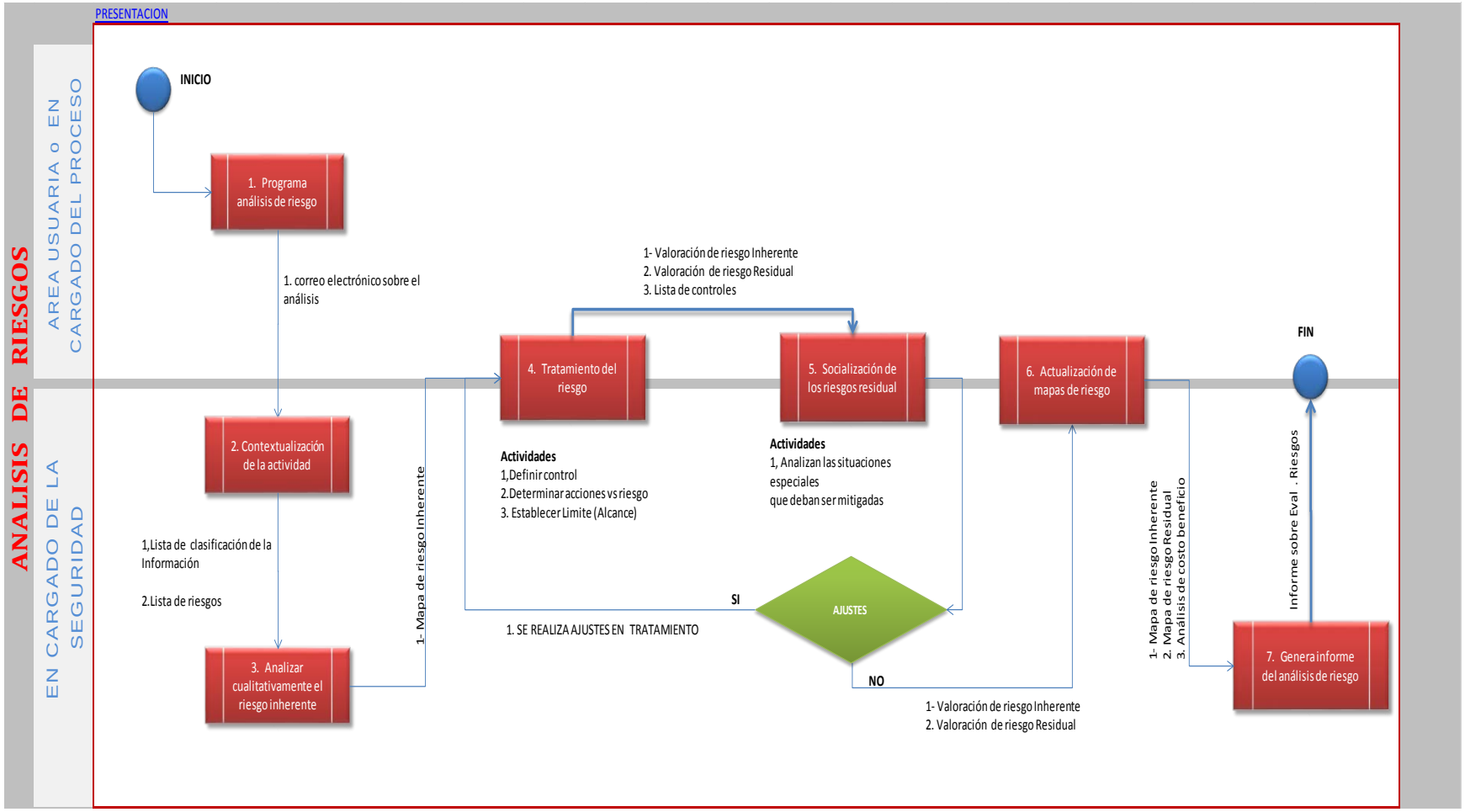


Figura 8 Proceso de análisis de riesgo

14. RESULTADOS Y DISCUSIÓN

Para validar el modelo expuesto en el presente proyecto, se llevaron a cabo dos pruebas piloto, aplicando las metodologías mediante entrevista a dos expertos de dos Mipymes diferentes[5]. A continuación se muestran los resultados de las pruebas efectuadas.

a) Resultados prueba piloto No. 1.

Para esta prueba se realizaron las entrevistas y la aplicación de los cuestionarios a un experto (Abogado titulado) de una mipyme de asesoría y representación legal, especializada en temas laborales y pensiones. De acuerdo a lo anterior, se realizaron los análisis que se presentan a continuación:

- **Metodología de diagnóstico de nivel de madurez**

  De acuerdo con la aplicación del cuestionario de nivel de madurez por dominio según la ISO 27002, se tuvieron los siguientes resultados:

EMPRESA: GESTION DE COBRO Y PROCESOS LEGALES		
RESULTADOS CONSOLIDADOS		**NIVEL DE MADUREZ Y CUMPLIMIENTO**
CALIFICACIÓN DEL NIVEL DE MADUREZ		**0,1**
5	Políticas de seguridad.	**0,0**
6	Aspectos organizativos de la seguridad de la información	**0,1**
7	Seguridad ligada a los recursos humanos	**0,2**
8	Gestión de activos	**0,0**
9	Control de accesos.	**0,1**
10	Cifrado	**0,0**
11	Seguridad física y ambiental.	**0,2**
12	Seguridad en la operativa	**0,1**
13	Seguridad en las telecomunicaciones	**0,0**
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	**0,0**
15	Relaciones con suministradores	**0,0**
16	Gestión de incidentes en la seguridad de la información.	**0,0**
17	Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio	**0,0**
18	Cumplimiento	**0,1**

Tabla 13. Resultados nivel de madurez prueba 2

[5] Por efectos de confidencialidad y reserva de información, los expertos entrevistados han solicitado que no se mencione el nombre de las firmas para las cuales trabajan, así como tampoco sus nombres.

Como se observa en la tabla, se obtuvo un puntaje de 0,1 que da como resultado, según la escala de evaluación que “No Existe”, lo anterior indica que en esta entidad no se ha reconocido siquiera que existe un problema a resolver.

De manera gráfica, a continuación se puede observar por dominio el nivel de calificación.

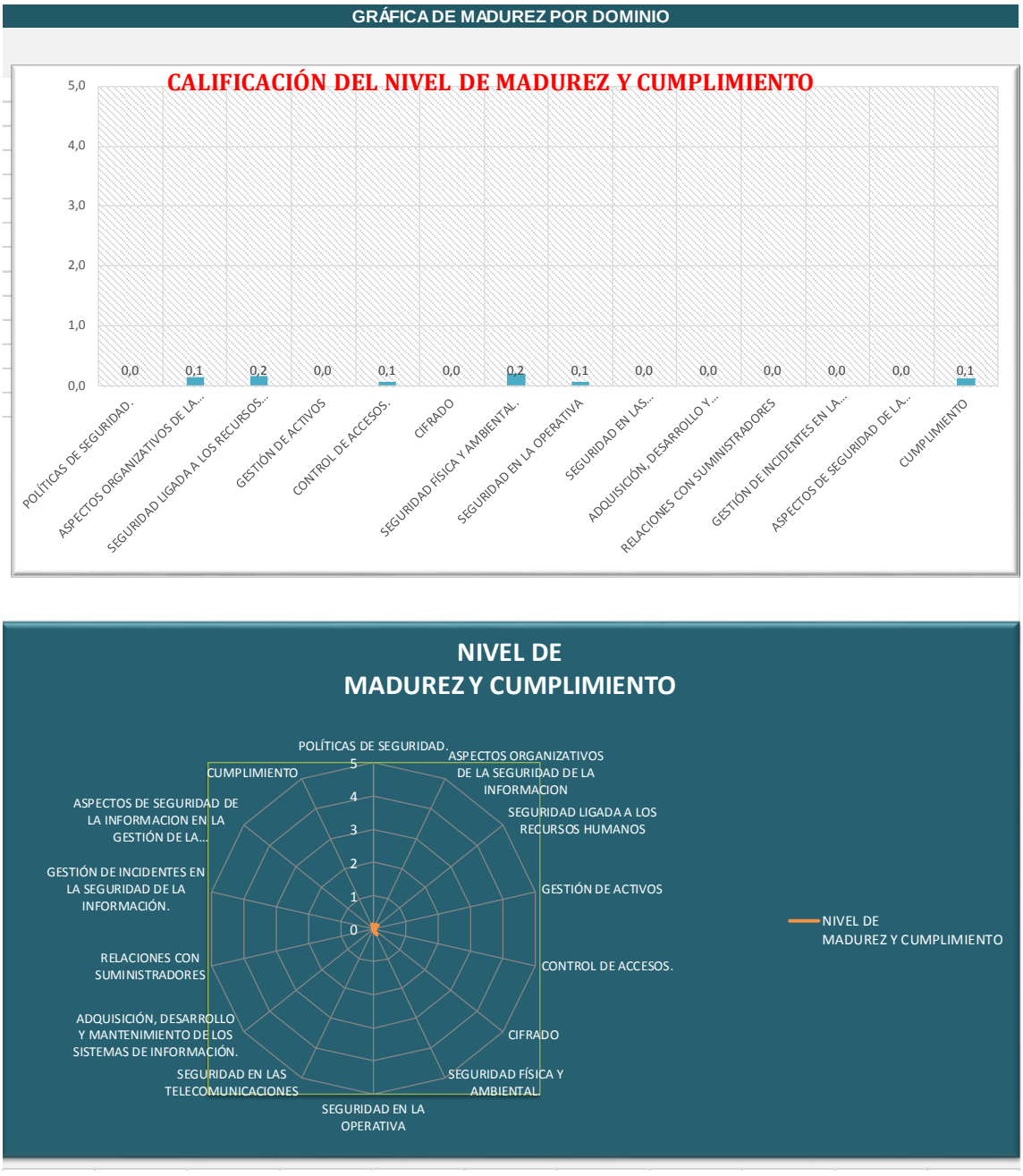


Figura 9 Grado de madurez Compañía2

Dentro del análisis general se pudo observar que esta entidad no cuenta con ningún modelo o sistema de Seguridad de la Información, por lo que en todos los dominios la calificación es baja o nula.

- **Metodología de identificación y clasificación de activos de información**

De acuerdo con lo planteado por el experto y a la aplicación de la metodología de identificación y clasificación de activos de información, se obtuvieron los siguientes resultados:

ETAPA I: Identificación e inventario de los activos de información

En esta etapa, el experto identificó los activos de información más relevantes y comunes en su empresa, dándoles su respectiva descripción y justificación.

Nombre del activo de información	Descripción del activo de información	Justificación del activo de información
Documento de información preliminar	Es el formato, grabación o cualquier medio donde queda registrada y evidenciada la información inicial que suministra el cliente al abogado.	Es usado para proteger la responsabilidad civil profesional del abogado
Contrato	Acuerdo de voluntad entre el cliente y la oficina en donde ambas partes aceptan las acciones y las condiciones para llevar a cabo la representación legal	Para formalizar por escrito los derechos y obligaciones de las partes y que se pueda resolver un eventual desacuerdo entre las partes.
Poder	Documento en el que el cliente otorga la facultad de representación legal a un abogado para adelantar los procesos legales correspondientes	Para adelantar trámites legales o administrativos en representación de un tercero
Evidencias	Documento que prueba la ocurrencia de un hecho	Para probar la ocurrencia de un hecho
Citación a conciliación	Documento generado por la procuraduría o mediante oficio directo que se debe notificar a la contraparte del proceso, lo cual se evidencia con un radicado en el documento.	Informar a la contraparte del proceso que se apertura
Fallo de la demanda	Documento que contiene la decisión definitiva del juez o tribunal competente.	Para exigir el cumplimiento de la sentencia en el caso eventual en que se incumpla

Tabla 14. Activos de información compañía 2

ETAPA II: Características de los activos de información

En esta etapa, se determinaron las características básicas de los activos de información identificados en la etapa anterior, donde se encontraron: contenedores, ubicación de los contenedores y custodios.

De acuerdo con el análisis efectuado, en su mayoría los activos de información se encuentran almacenados en 3 contenedores específicos:

- Archivadores
- Estaciones de trabajo
- Medios de almacenamiento extraíbles (USB – CD).

De igual forma, los responsables de los activos de información son:

- Los abogados
- La secretaria o asistente.

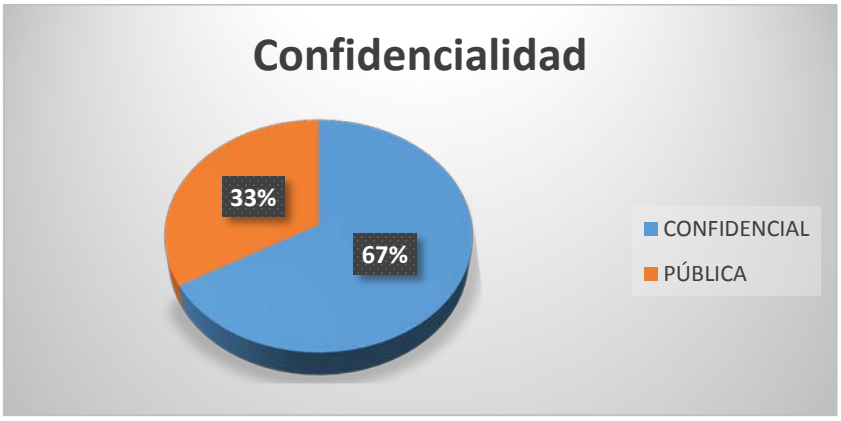
La información está siempre en las instalaciones de la empresa:

- Oficina de abogados (puestos de trabajo)
- Oficina secretaria (Puesto de trabajo)

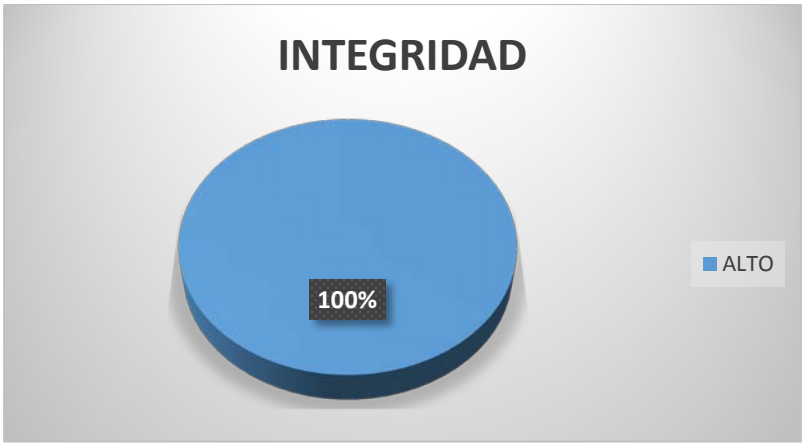
ETAPA III: Clasificación de Activos de Información

Para cada uno de los activos se determinó su clasificación de acuerdo con la metodología establecida.

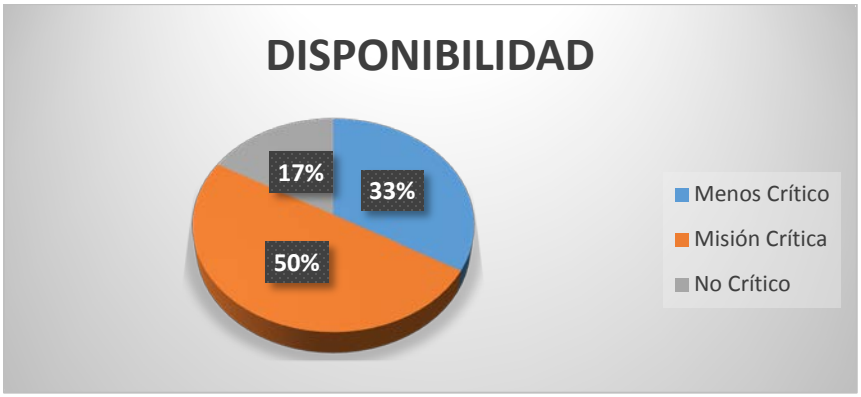
- **Confidencialidad**: De acuerdo con el análisis realizado con el experto y teniendo en cuenta las escalas definidas (activo de información de uso público, uso interno o confidencial) se observó que en su mayoría los activos de información identificados son confidenciales.



- **Integridad**: De acuerdo con las escalas definidas, según el impacto en caso de pérdida de integridad de la información (Impacto alto, medio o bajo) se observó que la mayoría de los activos de información identificados tienen un impacto “alto” en caso de pérdida de integridad.



- **Disponibilidad**: De acuerdo con el análisis realizado con el experto, de acuerdo con las escalas definidas (No crítico, menos crítico, misión crítica) se observó que el 50% los activos de información identificados tienen una disponibilidad nivel “misión crítica”.



- **Contenedores Críticos**: De acuerdo con la confidencialidad, integridad y disponibilidad de los activos identificados y analizados, todos son activos críticos para la entidad. Por lo tanto todos los contenedores que contienen dichos activos son de criticidad “Alta”.

Contenedor	Nivel de criticidad
Estaciones de trabajo	Alto
Archivadores	Alto
Medios de almacenamiento removibles	Alto

Tabla 15. Contenedores críticos compañía 2

b. Resultados prueba piloto No. 2.

Para esta prueba se realizaron las entrevistas y la aplicación de los cuestionarios a un experto (Asistente y Directivo) de una mipyme de asesoría y representación legal, especializada en cobro pre jurídico y jurídico de cartera castigada y derecho legal. De acuerdo a lo anterior, se realizaron los análisis que se presentan a continuación:

- **Metodología de diagnóstico de nivel de madurez**

  De acuerdo con la aplicación del cuestionario de nivel de madurez por dominio según la ISO 27002, se tuvieron los siguientes resultados:

EMPRESA 1 GESTION DE COBRO DE CARTERA		
RESULTADOS CONSOLIDADOS		**NIVEL DE MADUREZ Y CUMPLIMIENTO**
CALIFICACIÓN DEL NIVEL DE MADUREZ		**0,3**
5	Políticas de seguridad.	0,0
6	Aspectos organizativos de la seguridad de la información	0,6
7	Seguridad ligada a los recursos humanos	0,7
8	Gestión de activos	0,8
9	Control de accesos.	0,2
10	Cifrado	0,0
11	Seguridad física y ambiental.	0,3
12	Seguridad en la operativa	0,3
13	Seguridad en las telecomunicaciones	0,4
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	0,0
15	Relaciones con suministradores	0,4
16	Gestión de incidentes en la seguridad de la información.	0,1
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	0,0
18	Cumplimiento	0,6

Tabla 16. Resultados nivel de madurez prueba 1

Como se observa en la tabla, se obtuvo un puntaje de 0,3 (“Promedio de los dominios”) que da como resultado, según la escala de evaluación que “No Existe”, lo anterior indica que en esta entidad no se ha reconocido siquiera que existe un problema a resolver.

Aunque en los dominios: aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos y gestión de activos, tienen una tendencia una escala “Inicial” (1) ya que utilizan algunos tipos de control, pero no tienen el conocimiento del porque y para que de los controles que se encuentran implementados, solo se realiza como un actividad orientada a cumplir un requisito de la compañía, en algunos casos los empleados no tienen

conocimiento de la existencia de controles o medidas de permitan proteger los activos, finalmente no se evidenciaron procesos de monitoreo o mecanismo de medición para validar la efectividad y eficiencia de los controles. De manera gráfica, a continuación se puede observar por dominio el nivel de calificación.

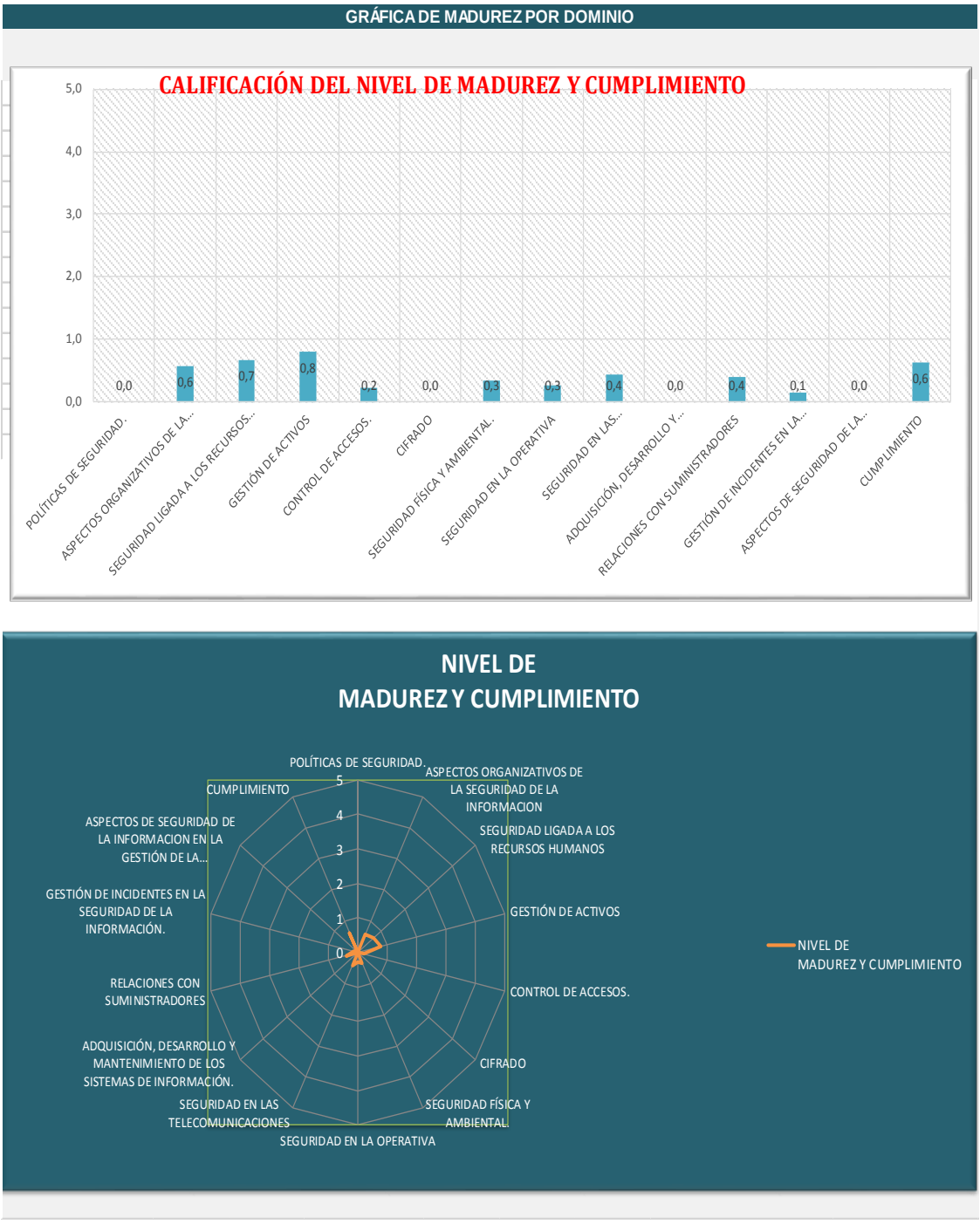


Figura 10 Grado de madurez Compañía1

- **Metodología de identificación y clasificación de activos de información**

De acuerdo con lo planteado por el experto y a la aplicación de la metodología de identificación y clasificación de activos de información, se obtuvieron los siguientes resultados:

ETAPA I: Identificación e inventario de los activos de información

En esta etapa, el experto identificó los activos de información más relevantes y comunes en su empresa, dándoles su respectiva descripción y justificación.

Nombre del activo de información	Descripción del activo de información	Justificación del activo de información
Contrato	Acuerdo de voluntad entre el cliente y la oficina en donde ambas partes aceptan las acciones y las condiciones para llevar a cabo la representación legal	Para formalizar por escrito los derechos y obligaciones de las partes y que se pueda resolver un eventual desacuerdo entre las partes.
Inventarios	Tipo de información que se encuentre en medio impreso y magnético de los activos físicos de la compañía	Llevar el seguimiento y el estado de los activos físicos de la compañía
Lista de proveedores	Tipo de información que se encuentre en medio impreso y magnético de la información de contacto de los proveedores de servicio de papelería, Equipos de cómputos	Tener conocimiento y clasificación de los mejores proveedores
Cartas de retiro	Tipo de información que se encuentre en medio impreso y magnético de la información de del retiro voluntario de los empleados	Tener el seguimiento de los recursos que realizan cambio de la compañía
Contabilidad	Tipo de información que se encuentre en medio impreso y magnético del estado financiero de la compañía	Información del estado económico de la compañía
Cuentas de Cobro	Tipo de información que se encuentre en medio impreso y magnético de los cobros a los clientes de las asesorías y servicios prestados	Información de la cuentas por cobrar
Lista de Clientes	Tipo de información que se encuentre en medio impreso y magnético de datos de contacto de los clientes	Tener conocimiento de los clientes y los perfiles
Información de Proceso	Documentos de los evidencias de los procesos como evidencias que prueba la ocurrencia de un hecho	Para probar la ocurrencia de un hecho
información Sensible de cobros	evidencias que prueba el proceso de cobranza realizada	Para probar la ocurrencia de un hecho
Información de CDT´s	Información de cobro de cdt pendientes por cobrar	Para probar la ocurrencia de un hecho

Tabla 17. Activos de información compañía 1

ETAPA II: Características de los activos de información

En esta etapa, se determinaron las características básicas de los activos de información identificados en la etapa anterior, donde se encontraron: contenedores, ubicación de los contenedores y custodios.

De acuerdo con el análisis efectuado, en su mayoría los activos de información se encuentran almacenados en 3 contenedores específicos:

- Estaciones de Trabajo
- Archivador
- Medio Magnético Extraíble

De igual forma, los responsables de los activos de información son:

- Directivo
- asesores
- secretaria
- abogados

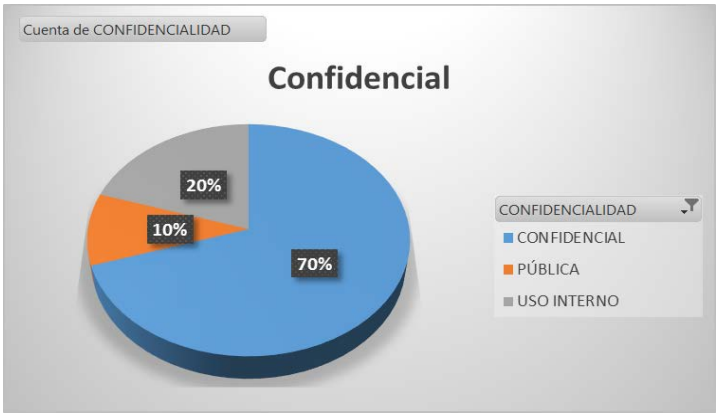
La información está siempre en las instalaciones de la empresa:

- Oficina (puestos de trabajo) en algunos casos los equipos portátiles de los abogados o asesores son retirados para su gestión.

ETAPA III: Clasificación de Activos de Información

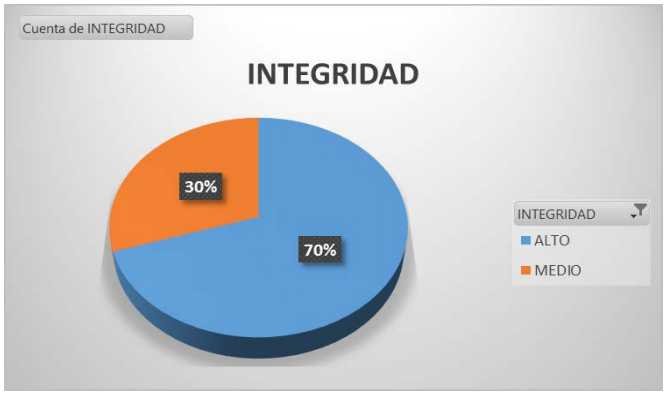
Para cada uno de los activos se determinó su clasificación de acuerdo con la metodología establecida.

- **Confidencialidad**: De acuerdo con el análisis realizado con el experto y teniendo en cuenta las escalas definidas (activo de información de uso público, uso interno o confidencial) se observó que en su mayoría los activos de información identificados son confidenciales.



- **Integridad**: De acuerdo con las escalas definidas, según el impacto en caso de pérdida de integridad de la información (Impacto alto, medio o bajo) se

observó que la 70% de los activos de información identificados tienen un impacto “Alto” en caso de pérdida de integridad.



- **Disponibilidad**: De acuerdo con el análisis realizado con el experto, de acuerdo con las escalas definidas (No crítico, menos crítico, misión crítica) se observó que en su mayoría los activos de información identificados tienen una Nivel sensible, dado que el 80% de los activos se clasificaron en una escala de “misión crítica” y “Misión menos critica” , lo cual indica que si la información no está disponible puede afectar legalmente , reputacióna l y económicamente a la compañía en una forma significativa.

- **Contenedores Críticos**: De acuerdo con la confidencialidad, integridad y disponibilidad de los activos identificados y analizados, todos son activos críticos para la entidad. Por lo tanto todos los contenedores que contienen dichos activos son de criticidad “Alta”.

Contenedor	Nivel de criticidad
Estaciones de trabajo	Alto
Archivadores	Alto
Medios de almacenamiento removibles	Alto

Tabla 18. Contenedores críticos compañía 1

- **Metodología de análisis e identificación de riesgos**

Para exponer los resultados de la metodología de análisis e identificación de riesgos, es necesario aclarar que se aplicaron de forma unificada los criterios de análisis y parámetros de evaluación de riesgos, aunque utilizando dos fuentes de información diferentes (prueba piloto 1 y prueba piloto 2).

En las dos pruebas piloto, como se mencionó en la etapa anterior, se identificaron los siguientes contenedores de información crítica:

- ✓ Estaciones de trabajo
- ✓ Archivadores
- ✓ Medios de almacenamiento removibles

ETAPA I y II:

A cada uno de los contenedores se les realizó el análisis de amenazas, vulnerabilidades que aplicaban según cada caso. De dicho análisis se determinaron los siguientes riesgos:

- Estaciones de trabajo:
  - ✓ Posible compromiso de la disponibilidad de la información o interrupción de las actividades
  - ✓ Posible pérdida de información por fallas en el sistema eléctrico.
  - ✓ Posible interrupción de las actividades o potencial falla de los sistemas
  - ✓ Posible compromiso de la integridad del software o de la información
  - ✓ Posible interrupción de las actividades o potencial pérdida, daño, hurto o compromiso de los activos
  - ✓ Posible compromiso de la confidencialidad, la integridad y la disponibilidad de la información
  - ✓ Posible ejecución de actividades no autorizadas en los activos de información
  - ✓ Posible acceso no autorizado a información confidencial
  - ✓ Posible falta de gestión de la seguridad de la información dentro de la organización
  - ✓ Posible falta de protección sobre los activos de información
  - ✓ Posible divulgación, modificación o destrucción no autorizada de información o interrupción de las actividades
  - ✓ Posible compromiso de la confidencialidad por parte del personal que se desvincula o cambia su relación laboral
  - ✓ Posible error humano, falta de conciencia o incumplimiento de la política de seguridad en las actividades diarias
  - ✓ Posible error, pérdida, modificación no autorizada, vulnerabilidad técnica o fuga de información

- ✓ Posible compromiso de la confidencialidad de la información que se intercambia interna y externamente

- Medios de almacenamiento removibles

  - ✓ Posible interrupción de las actividades o potencial pérdida, daño, hurto o compromiso de los activos
  - ✓ Posible compromiso de la disponibilidad de la información o interrupción de las actividades
  - ✓ Posible interrupción de las actividades o potencial pérdida, daño, hurto o compromiso de los activos
  - ✓ Posible compromiso de la confidencialidad, la integridad y la disponibilidad de la información
  - ✓ Posible falta de protección sobre los activos de información
  - ✓ Posible divulgación, modificación o destrucción no autorizada de información o interrupción de las actividades
  - ✓ Posible falta de protección de la información confidencial
  - ✓ Posible error, pérdida, modificación no autorizada, vulnerabilidad técnica o fuga de información
  - ✓ Posible falta de gestión de la seguridad de la información dentro de la organización
  - ✓ Posible error humano, falta de conciencia o incumplimiento de la política de seguridad en las actividades diarias
  - ✓ Posible compromiso de la confidencialidad por parte del personal que se desvincula o cambia su relación laboral
  - ✓ Posible acceso no autorizado a información confidencial

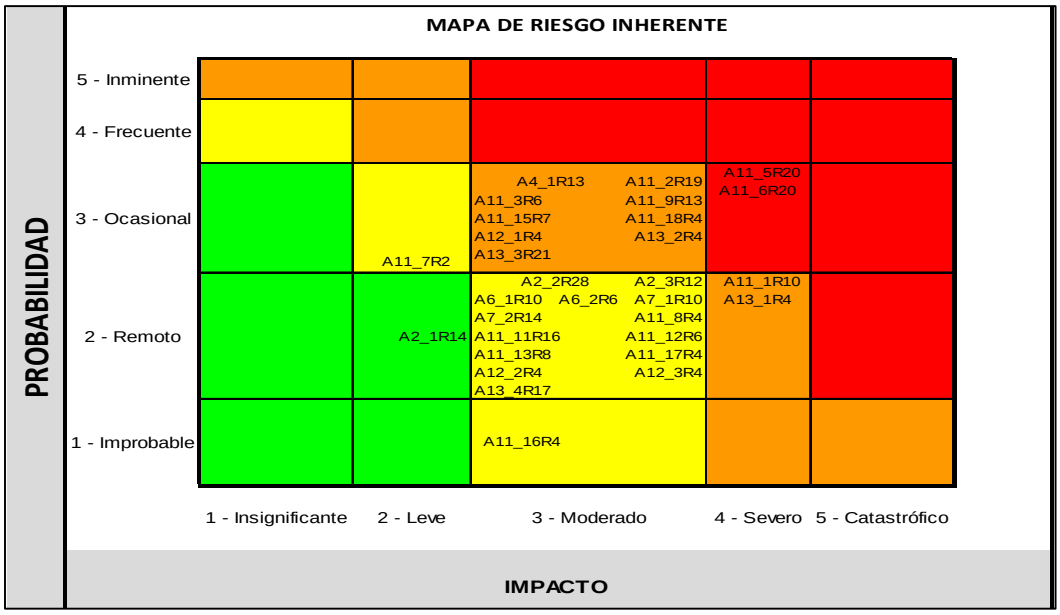
- Archivadores

  - ✓ Posible interrupción de las actividades o potencial pérdida, daño, hurto o compromiso de los activos
  - ✓ Posible acceso físico no autorizado, o daños e interferencias contra las instalaciones y la información
  - ✓ Posible falta de gestión de la seguridad de la información dentro de la organización
  - ✓ Posible falta de protección de la información en redes o infraestructura tecnológica
  - ✓ Posible interrupción de las actividades o potencial falla de los sistemas
  - ✓ Posible acceso no autorizado a información confidencial
  - ✓ Posible falta de protección sobre los activos de información
  - ✓ Posible compromiso de la confidencialidad de la información que se intercambia interna y externamente
  - ✓ Posible error humano, falta de conciencia o incumplimiento de la política de seguridad en las actividades diarias

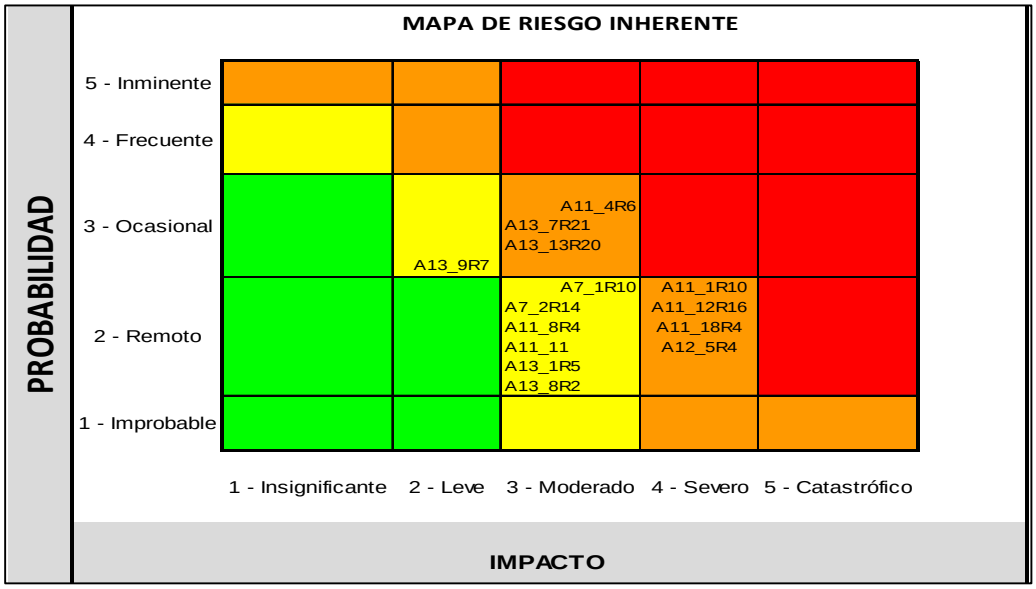
ETAPA III, IV Y V

Por cada una de los riesgos según su la amenaza o vulnerabilidad, se realizó el análisis de impacto por probabilidad para identificar el nivel del riesgo. Los mapas de calor donde se observan los riesgos inherentes, muestran los siguientes resultados por contenedor[6]:

- ✓ Estaciones de trabajo:

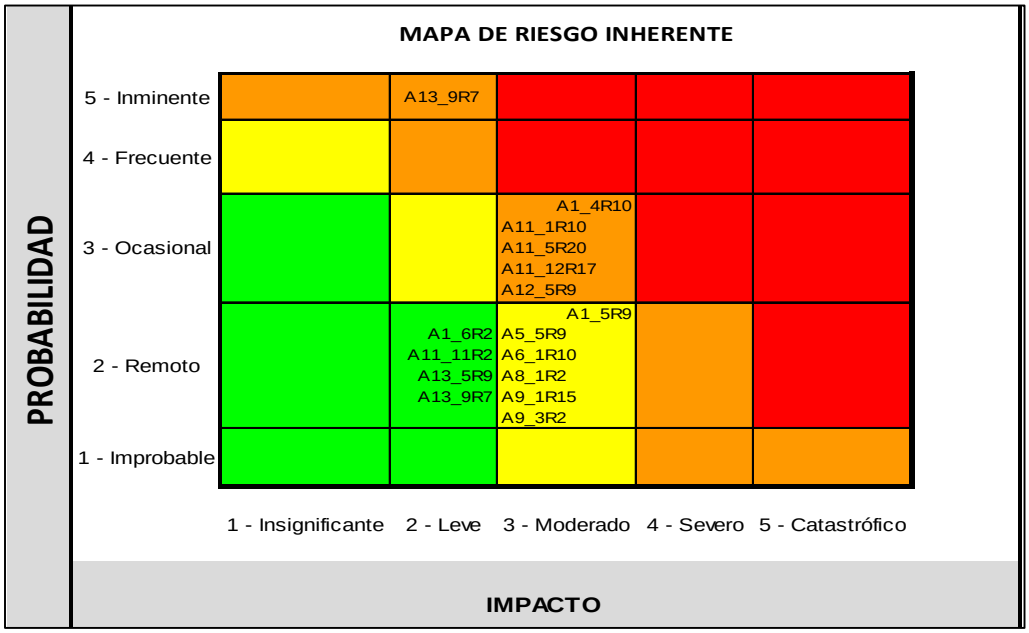


- ✓ Medios de almacenamiento removibles:



[6] Para mayor información, ver el archivo anexo donde se observa más detalladamente cada análisis y resultado obtenido.

- ✓ Archivadores



ETAPA VI

En esta etapa se presenta el tratamiento del riesgo y los controles que los autores recomiendan para el tratamiento de los riesgos por contenedor, contemplando los objetivos de control de la ISO 27002. Es importante mencionar que se realizó el análisis para los riegos calificados como “altos” y “Extremos”, esto considerando que son los que requieren más prioridad en su tratamiento.

Cabe resaltar que, este tratamiento dependerá del apetito y tolerancia al riesgo que cada entidad desea asumir.

Los controles son los siguientes, según el contenedor:

- **Estaciones de trabajo:**

  - ✓ Implantar controles para la detección, prevención y recuperación de software malicioso.
  - ✓ Se debe identificar los privilegios asociados a las cuentas de acceso a los sistemas y aplicaciones utilizados, con base a una clasificación basada en una codificación alfanumérica que permita describir la clasificación del tipo de Cargo, el área/gerencia a la que pertenece y la relación con el cargo al que será asignado el perfil.
  - ✓ La matriz de perfiles y funciones debe garantizar la separación de funciones vs los permisos autorizados sobre los activos de infraestructura de cómputo, sistemas operativos, redes y comunicaciones, así como por cada una de las aplicaciones a las que tenga autorizado el acceso su función.

- ✓ Las contraseñas se deben memorizar y almacenar de forma segura de tal manera que nadie más pueda conocerlas. Las contraseñas no deberán almacenarse en archivos no estructurados, en texto claro, escritos en papeles, o en medios que puedan ser leídos por terceros.
- ✓ Implementar controles automáticos y/o manuales que permiten identificar y prevenir la fuga de información (ej. Implementación Data Lost Prevention para controlar la fuga de información privada /confidencial fuera de la organización) por medio de USB, quemadores de CD – DVD y/o a través del envío de información por los diferentes medios de internet (mensajería instantánea, correo electrónico, cargar información en foros o portales entre otros).
- ✓ Todos los empleados de la Entidad, cuando sea pertinente los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre políticas y los procedimientos del Entidad, según sea pertinente.
- ✓ Todos los archivos provenientes de dispositivos “USB”, CD, DVD, o anexos en correos electrónicos y que se requieran copiar en la red de la Firma, deben ser examinados con software antivirus antes de usarlos. En caso que los archivos descargados estén cifrados y comprimidos, deben descifrarse y descomprimirse antes de ser sometidos a la verificación antivirus.
- ✓ Implementar mecanismos de cifrado de información para proteger la información que se tiene en los dispositivos móviles, para proteger la información sensitiva por extravío o robo de información.
- ✓ De ser posible, se deben bloquear los puertos USB y quemadores de CD - DVD de los equipos de los empleados de la Firma para prevenir la fuga de información. En el caso que no sea posible, se debe implementar unos agentes que monitoreen y/o bloqueen las copias de información confidencial /privada en dichos dispositivos.
- ✓ Definir requerimientos para el almacenamiento de los respaldos de datos dentro (onsite) y fuera (offsite) del sitio, de acuerdo con las necesidades del negocio.
- ✓ Los reportes generados por cualquier aplicativo, contendrán la información referente a las fallas que serán monitoreadas diariamente y se analizarán en el menor tiempo posible para tomar las acciones correctivas pertinentes y así poder dar solución pronta al problema o problemas que presenten.
- ✓ Establecer y comunicar políticas y procedimientos para la identificación, autenticación y autorización de accesos para todos los usuarios que necesiten consultar, manipular, registrar, validar la información del negocio contenida en los sistemas.
- ✓ Como medida de prevención de riesgos a la información, se deben implementar los horarios de acceso a la información privilegiada de la Firma, delimitándolas al horario laboral de los trabajadores y manteniendo el registro de los movimientos de acceso a la información de los usuarios autorizados con el detalle de los tiempos de acceso y salida, así como también del uso a dicha información.
- ✓ Según el rol de usuario se debe restringir el tamaño o la posibilidad de adjuntar archivos en los correos.

- **Medios de almacenamiento removibles**

  - ✓ Establecer acuerdos legales, regulatorios y requerimientos de negocios para almacenar y conservar documentos, datos, archivos, programas, reportes y mensajes.
  - ✓ Implementar mecanismos de cifrado de información para proteger la información que se tiene en los dispositivos móviles, para proteger la información sensitiva por extravío o robo de información.
  - ✓ Los administradores que operan las solicitudes de altas, bajas y cambios de usuarios deben revisar si están correctamente definidos y asignados los permisos, a pesar de ser autorizados por los Gerentes o titulares de las diferentes áreas, de acuerdo a la matriz de perfiles y funciones. Si hubiere alguna duda, tendrán que activar los permisos que están correctos y los que haya duda o estén mal asignados deberán ser comentados con los que autorizaron el requerimiento para identificar la necesidad. Si no existe una justificación clara, el caso debe ser escalado según el procedimiento que se tenga definido para determinar qué acciones se deben seguir, si se crea o se actualizan los perfiles autorizados. Todo requerimiento debe estar formalmente autorizado y requerido.
  - ✓ La matriz de perfiles y funciones debe garantizar la separación de funciones vs los permisos autorizados sobre los activos de infraestructura de cómputo, sistemas operativos, redes y comunicaciones, así como por cada una de las aplicaciones a las que tenga autorizado el acceso su función.
  - ✓ Se debe identificar los privilegios asociados a las cuentas de acceso a los sistemas y aplicaciones utilizados, con base a una clasificación basada en una codificación alfanumérica que permita describir la clasificación del tipo de Cargo, el área/gerencia a la que pertenece y la relación con el cargo al que será asignado el perfil.
  - ✓ Como medida de prevención de riesgos a la información, se deben implementar los horarios de acceso a la información privilegiada de la Firma, delimitándolas al horario laboral de los trabajadores y manteniendo el registro de los movimientos de acceso a la información de los usuarios autorizados con el detalle de los tiempos de acceso y salida, así como también del uso a dicha información.

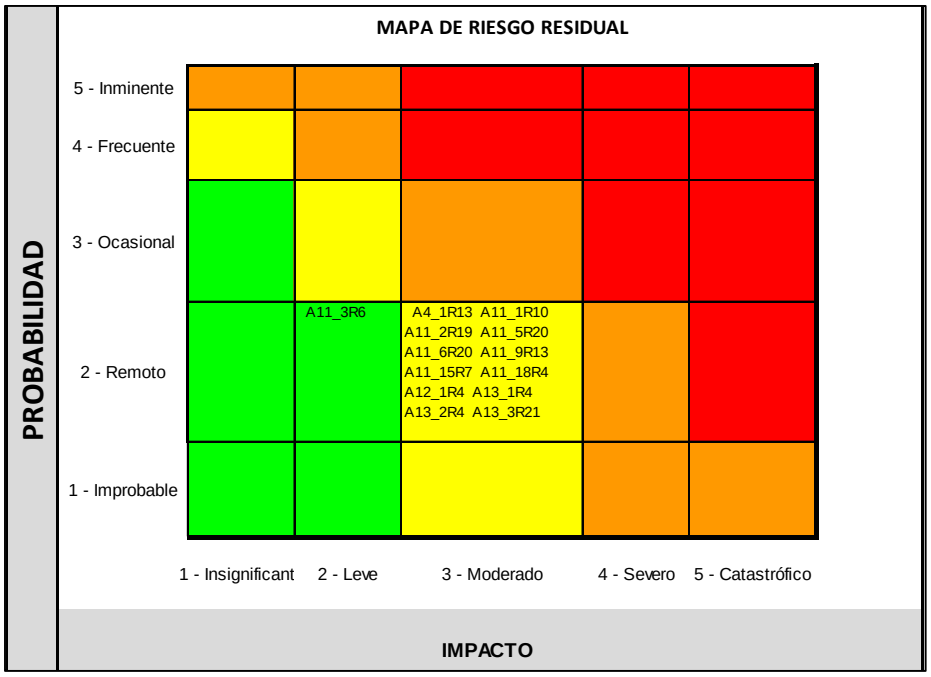
- **Archivadores**

  - ✓ Diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones
  - ✓ Diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras
  - ✓ La información que es distribuida físicamente y enviada por correo interno/externo debe ser identificada claramente como información confidencial y sellada de tal forma, que si la abren antes de llegar al destinatario, el mismo puede identificar que la información pudo haber sido alterada y/o leída por personal no autorizado. En caso que de que estas situaciones se presenten, se debe informar la situación al área de seguridad para que se realicen las respectivas investigaciones.

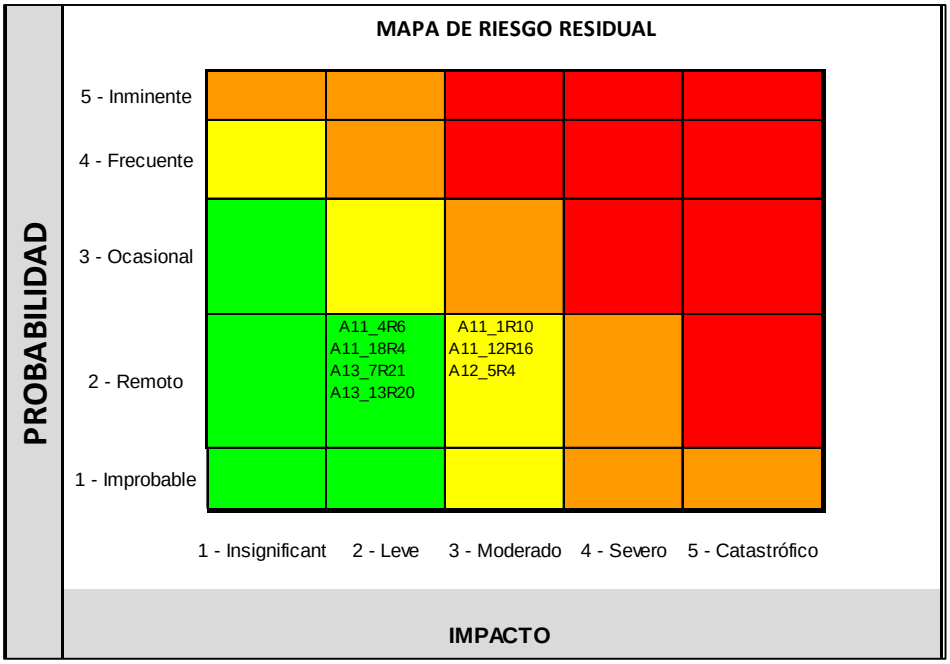
- ✓ La información privada/confidencial no puede ser almacenada en escritorios y/o lugares sin ningún control de acceso físico.
- ✓ La información privada/confidencial que debe permanecen en las oficinas de la Firma debe ser almacenada en archivos, cajas fuertes, gavetas con un acceso físico, ya sea una tarjeta de proximidad, una llave y/o una contraseña. El lugar de almacenamiento y su control de acceso depende lo sensitiva que sea la información.
- ✓ Como medida de prevención de riesgos a la información, se deben implementar los horarios de acceso a la información privilegiada de la Firma, delimitándolas al horario laboral de los trabajadores y manteniendo el registro de los movimientos de acceso a la información de los usuarios autorizados con el detalle de los tiempos de acceso y salida, así como también del uso a dicha información.

Los riesgos inherentes que quedarían si se implementan los controles mencionados en la punto anterior se registran de la siguiente manera:

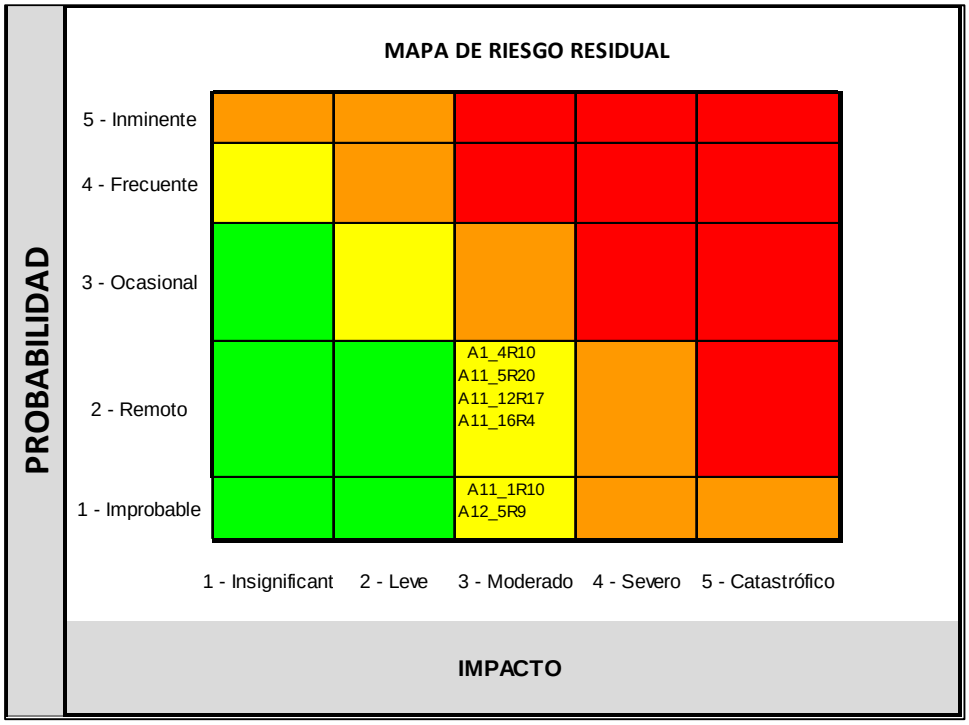
Estaciones de trabajo:



Medios de almacenamiento removibles



Archivadores



15. CONCLUSIONES Y RECOMENDACIONES

- Al diseñar y aplicar las metodologías expuestas en este documento, se puede concluir que de esta forma se hace una primera aproximación a la aplicación de un sistema de Gestión de Seguridad de la Información, no sólo en empresas de asesoría legal, sino que también se sienta un precedente para implementarlo en Mipymes de otros sectores en Colombia.

- Se recomienda que aquellas empresas de asesoría legal que opten por implementar las metodologías planteadas en este documento, efectúen una revisión y verificación de los posibles cambios que puedan haber surgido en la norma ISO 27002 (asociados a una actualización de la norma internacional) para garantizar que su aplicabilidad incluye todos los frentes de análisis de Seguridad de la Información.

- Se obtuvieron importantes resultados que permiten inferir que el estado de avance y madurez en temas de SI en Mipymes de asesoría legal no es muy avanzado aún. Se evidenció que se tienen debilidades en la protección a la información que manejan estas empresas.

- Dado que las mipymes de asesoría legal tienen una muy estrecha relación con el sistema Judicial Colombiano, específicamente con Juzgados y tribunales, se hace imperativo que proyectos como este, se enfoquen a mejorar el avance en Seguridad de la Información de todo el sector judicial, no sólo en las mipymes o empresas privadas, sino también que se permita su aplicación en los entes administradores de justicia. Se recomienda entonces, que el Estado Colombiano comprenda la importancia de la SI y promueva la implementación de estas metodologías en entidades estatales.

- Dado que la mayor parte de información que se maneja en estas mipymes es confidencial, es preciso implementar cuidados especiales para conservar su integridad y garantizar que sólo accedan las personas autorizadas. En este trabajo se plantearon controles para mitigar estos riesgos, pero cada empresa deberá diseñar sus controles propios o bien ajustar los aquí propuestos.

- Es importante que cada entidad personalice las metodologías planteadas en este trabajo de acuerdo con sus objetivos de negocio y necesidades específicas. Se debe considerar el apetito del riesgo que determine cada empresa y a partir de esto analizar riesgos y controlarlos.

- Las entidades deben considerar un proceso donde se incluya una revisión, monitoreo y evaluación del nivel de madurez de la seguridad de la información de forma periódica.

- Se observó que hay muchos controles básicos, a nivel de accesos lógicos y físicos que estas entidades pueden implementar sin tener que incurrir en altos costos y que permiten de una manera básica proteger los activos de información.

16. BIBLIOGRAFÍA

[1] ISO/IEC 27000 , «Information technology - Security techniques - Information security management systems - Overview and vocabulary" International Organization for Standarization (ISO),» de *Information security management systems*, p. http://www.iso.org/.

[2] ISO/IEC, «ISO/IEC 20000-2:2013, Information technology — Service management — Part 2: Guidance on the application of service management systems.».

[3] iso27000, «Copyright © All Rights Reserved Free Website Template By: PriteshGupta.com,» 2012, p. http://www.iso27000.es/iso27002_5.html#home.

[4] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT – versión 3.0, Madrid, octubre de 2012, pp. https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.1/web/magerit/Libro_I_metodo.pdf.

[5] c063411_ISO_IEC_27000_2014.pdf, «techniques — Information security management systems — Overview and vocabulary,» de *INTERNATIONAL STANDARD ISO/IEC 27000*, Third edition 2014-01-15.

[6] IT Governance Institute, «MODELO DE MADUREZ,» de *COBIT 4.1*, cobiT4.1spanish.pdf, 2007, p. www.itgi.org.

17. ANEXOS

- *01_EvaluacionCompañiasV3.xlsx*
- *02_DiagramasProcesos3.xlsx*
- *03_ValoraciónActivos.xlsx*
- *04_Analisis_RiesgosV5.xlsm*