MODELO DE MADUREZ PARA LA SEGURIDAD DE LA INFORMACIÓN

JUAN DAVID HENAO MONTOYA
200010197010
JUAN CAMILO LOPERA DIAZ
200017003010

UNIVERSIDAD EAFIT
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2007

MODELO DE MADUREZ PARA LA SEGURIDAD DE LA INFORMACIÓN

JUAN DAVID HENAO MONTOYA
JUAN CAMILO LOPERA DIAZ

Trabajo de Grado para Optar al Título de
Ingeniero de Sistemas

Asesor
RAFAEL DAVID RINCÓN B.
Magíster en Matemáticas Aplicadas
Magíster en Sistemas de Calidad

UNIVERSIDAD EAFIT
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2007

AGRADECIMIENTOS

Los autores de este Proyecto de Grado desean expresar un agradecimiento a las siguientes personas que colaboraron durante todo el proceso de elaboración, revisión y culminación de este trabajo:

A Dios y a nuestras familias que nos apoyaron incondicionalmente durante todo nuestro proceso de formación y en los momentos más difíciles de nuestras vidas, además de acompañarnos también en los mejores momentos.

A nuestro asesor Rafael David Rincón por el apoyo, colaboración y dedicación durante el desarrollo de este proyecto.

A la empresa REIMPEX S.A a su gerente Alvaro René Herrera Arango y a la jefa de sistemas Ingeniera Diana Patricia López por brindarnos el espacio, tiempo y conocimiento para evaluar el proyecto de grado.

A los jurados por sus valiosos aportes con los cuales contribuyeron a mejorar el presente trabajo.

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Si nos remontamos a la época que precedió a la revolución industrial, encontraríamos que las empresas producían lo que quisieran y como lo quisieran, sin tener en cuenta factores de calidad, satisfacción del cliente y mucho menos, cuidados necesarios con el medio ambiente; el cliente debía comprar lo que las grandes empresas producían pues no había nada más para escoger. Luego se presentó la libre competencia, donde a pesar de que se omitían factores claves de producción, los clientes tenían un mayor mercado de donde escoger, lo que obligó a las grandes empresas a preocuparse más por la satisfacción del cliente y entrar en una batalla por ofrecer calidad y un mejor precio.

En la actualidad, las preocupaciones de las organizaciones no solo se basan en la satisfacción del cliente y en ofrecer un buen precio, también requieren cumplir con unas normas legales, sanitarias y ambientales, que día a día se hacen más estrictas y conllevan unas altas sanciones al momento de no ser cumplidas; fuera de esto, la globalización obliga a las empresas a cumplir con unas normas internacionales para poder comercializar los bienes y servicios que producen para el exterior. Por todo lo anterior, más que un requerimiento, es una obligación para las organizaciones conocer el estado actual de sus procesos desde diferentes puntos de vista, tales como, efectividad de controles, calidad de la infraestructura tecnológica, planes de continuidad del negocio, etc. y proteger lo que hoy en día se considera lo más importante para una organización, su INFORMACIÓN.

Actualmente, las empresas toman las decisiones basadas en la información alojada en sus bases de datos y en el comportamiento del entorno, además, poseen información confidencial de clientes, proveedores y competidores, que se debe proteger contra posibles alteraciones, pérdidas, accesos no autorizados y estar disponible cada vez que se requiera. La combinación de estos factores crea la necesidad de implementar herramientas y metodologías que garanticen la seguridad de la información, y lograr de esta manera, cumplir con las premisas de confidencialidad, integridad y disponibilidad, propuesta por las mejores prácticas de seguridad. Sin embargo, esta implementación no se hace fácil dentro de las organizaciones debido a factores humanos, tecnológicos y de

costos, tales como poca cultura de riesgo, altos costos de dispositivos, proliferación de ataques, fuga de información, entre otras.

Por lo anterior, y reconociendo las necesidades que tienen las empresas de evaluar sus procesos y garantizar la seguridad de la información, se ha resuelto elaborar un modelo de madurez soportado en las mejores practicas internacionales como lo son la norma ISO 17799, la herramienta CoBit y el modelo CMMI, desarrollado por niveles de madurez que permitirán identificar la evolución de los procesos de TI, la evaluación e identificación de riesgos, la implementación de controles, entre otros factores que se deben tener en cuenta al momento de realizar un valoración del estado actual de la seguridad de la información, y lograr de esta manera ofrecerle a las empresas una herramienta que satisface sus necesidades frente a la evaluación de la seguridad de la información, la cual permitirá identificar los puntos en los que la empresa presenta debilidades y en cuales posee fortalezas o cumplen a cabalidad.

OBJETIVOS

1 OBJETIVO GENERAL

Desarrollar un modelo de madurez basado en el modelo CMMI (*Capability Maturity Model Integration*) que permita evaluar el estado actual de una compañía respecto a la seguridad de la información.

2 OBJETIVOS ESPECÍFICOS

- Elaborar una lista de chequeo basada en las mejores prácticas, los modelos y normas internacionales de seguridad, como lo son las ISO 17799 y CoBit versión 3, desarrolladas para evaluar la seguridad de la información.

- Presentar una clasificación por niveles, donde se permita ubicar el estado en que se encuentra la organización actualmente.

- Evidenciar las falencias que se obtuvieron posterior a la evaluación para facilitar sus acciones correctivas.

MARCO TEÓRICO

3 MODELO CMMI [1]

El modelo CMMI (*Capability Maturity Model Integration*) desarrollado por el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon (SEI), es un modelo de procesos que permite identificar el nivel de madurez de una organización basándose en la capacidad de sus procesos, con el fin de facilitar y simplificar la adopción de varios modelos de forma simultánea, tales como:

- CMM-SW (*CMM for Software*)
- SE-CMM (*Systems Engineering Capability Maturity Model*)
- IPD-CMM *(Integrated Product Development*)

El modelo CMMI tiene dos tipos de representaciones: continua y escalonada. Estas dos representaciones son equivalentes y las organizaciones pueden optar por la mejor que se adapte a sus características y prioridades de mejora.

La representación continua tiene como objetivo el nivel de capacidad de cada una de las áreas de proceso del modelo, mientras que la representación escalonada evalúa la madurez de la organización basándose en etapas definidas.

A continuación se presenta la relación que existe entre la representación Continua y la representación Escalonada, con las áreas de procesos que hacen parte de las organizaciones:

La representación continua está conformada por 6 niveles de capacidad, los cuales son:

- Nivel 0.- Incompleto: El proceso no se realiza, o no se consiguen sus objetivos.
- Nivel 1.- Ejecutado: El proceso se ejecuta y se logra su objetivo.
- Nivel 2.- Gestionado: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos.

[1] *www.sei.cmu.edu/cmmi*

- Nivel 3.- Definido: Además de ser un proceso "gestionado" se ajusta a la política de procesos que existe en la organización, alineada con las directivas de la empresa.
- Nivel 4.- Cuantitativamente gestionado: Además de ser un proceso definido, se controla utilizando técnicas cuantitativas.
- Nivel 5.- En optimización: Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica para adaptarlo a los objetivos del negocio.

La representación escalonada permite ubicar en qué lugar se encuentra la organización en uno de los 5 niveles de madurez en los que está distribuido el modelo. Estos niveles son:

- Nivel 1: Inicial. Los resultados de calidad obtenidos en el proceso de software son impredecibles, sin control, reactivo y son consecuencia de las personas y de las herramientas que emplean. Este nivel no depende de los procesos previamente definidos por la organización, ya que estos no existen o no son utilizados.

- Nivel 2: Gestionado. Se considera un nivel 2 de madurez cuando se llevan a cabo prácticas básicas de gestión de proyectos (costos, cronograma, funcionalidad), de gestión de requisitos, control de versiones y de los trabajos realizados por subcontratistas. Los equipos de los proyectos pueden aprovechar las prácticas realizadas para aplicarlas en nuevos proyectos.

- Nivel 3: Definido. Los procesos comunes para desarrollo y mantenimiento del software están documentados de manera suficiente en una biblioteca accesible a los equipos de desarrollo. Las personas han recibido la formación necesaria para comprender los procesos.

- Nivel 4: Gestionado cuantitativamente. La organización mide la calidad del producto y del proceso de forma cuantitativa con base en métricas establecidas. La capacidad de los procesos empleados es previsible, y el sistema de medición permite detectar si las variaciones de capacidad exceden los rangos aceptables para adoptar medidas correctivas.

- Nivel 5: En optimización. La mejora continua de los procesos afecta a toda la organización, que cuenta con medios para identificar las debilidades y reforzar la prevención de defectos. Se analizan de forma sistemática datos relativos a la eficacia de los procesos de software para analizar el coste y el beneficio de las adaptaciones y las mejoras. Se evalúan e implementan tecnologías innovadoras, buscando la mejora continua de los procesos.

4 SEGURIDAD DE LA INFORMACIÓN [2]

4.1 DEFINICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

"La Norma ISO/IEC 17799: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, se puede definir como un conjunto de políticas, normas, procedimientos y dispositivos físicos que involucran a personas, procesos y tecnologías (Figura 1), con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de los medios de procesamiento."

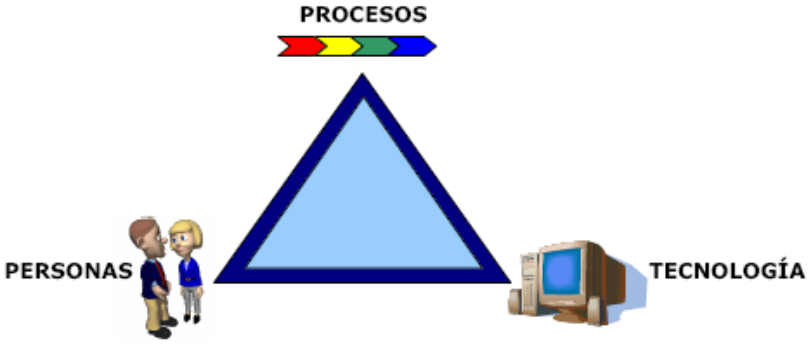

Figura 1. Triada Seguridad de la información
Fuente: "Hacia un Modelo de Madurez para la Seguridad de la Información"[3]

En la Figura 2 se muestra que la seguridad de la información se caracteriza por la preservación de su Confidencialidad, su Integridad y su Disponibilidad (Modelo CIA), teniendo en cuenta las necesidades del negocio para proteger esta información.

[2,3] *Barrientos A. Andrea Marcela, Aleiza C. Karen Alexandra,INTEGRACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON UN SISTEMA DE GESTIÓN DE LA CALIDAD, Proyecto de Grado, Universidad EAFIT, 2005.*

Figura 2. Elementos de la seguridad de la Información
Fuente: Adaptado de Appluscorp. Costa Rica, 2004

Para entender con mayor precisión la figura 2, la explicación de cada uno de sus elementos, es la siguiente:

4.2 MODELO CIA

El CIA (*Certified Internal Auditor*) es la certificación que concede el IIA (*Institute of Internal Auditors*) a los auditores que aprueban los 4 exámenes diseñados para tal fin. El CIA se estableció en el año 1941, y su sede principal está ubicada en Altamonte Springs, FLA, Estados Unidos, actualmente cuenta con más de 128.000 miembros.

Uno de los cuatro exámenes que se tienen diseñados para obtener la certificación CIA esta diseñado con énfasis en los sistemas de información. En este apartado se evalúan conocimientos en temas como:

- La planeación de la auditoría de TI y análisis de trabajos realizados previamente por la auditoría.
- Manejo de información y asignación de responsabilidades.
- Evaluación en centro de cómputo.
- Auditorías de sistemas operativos y software de administración de red.
- Evaluación de los sistemas de información.
- Auditorías de desarrollo de sistemas.
- Auditorías de telecomunicaciones y redes.
- Uso de herramientas asistidas por computadores (TAAC´s),

Este diseño de examen buscar medir el conocimiento de los auditores sobre los conceptos fundamentales de la seguridad de la información para preservar los pilares que la soportan: Confidencialidad, Integridad y Disponibilidad de la información. Estos conceptos se describen a continuación:

- **Confidencialidad**. Se refiere a que la información pueda ser accedida sólo por aquellas personas que están autorizadas para ello.

- **Integridad.** Se refiere a la exactitud y totalidad (completitud) de la información y de los medios de procesamiento**.**

- **Disponibilidad.** Se refiere a que los usuarios autorizados puedan acceder a la información y a los recursos relacionados con la misma, todas las veces que lo requieran.

4.3 GESTIÓN DE LA SEGURIDAD

La gestión de la seguridad involucra tres ámbitos: la organización, el entorno físico y el entorno lógico.

4.3.1 Organización

Un sistema de información en una organización formará parte de su infraestructura, modificando las formas de trabajar y las relaciones interpersonales, constituyéndose en una parte de alto riesgo dentro de dicha organización. Por ello, los directivos deben desempeñar un papel promotor y de animación en materia de seguridad, aplicando un plan estratégico de seguridad, que dé lugar a reglamentos de régimen interior en materia de seguridad, plan de contingencia y plan de seguridad informática. Todo esto requerirá, por supuesto, la implicación de todo el personal, debiendo dedicar una especial atención a la información y a la formación. Las responsabilidades de todo el personal con respecto a la seguridad deberán estar claramente definidas, al igual que la coordinación entre los responsables. Así, debería existir un servicio o sección de seguridad vinculado a una Dirección General independiente. También deberá disponerse de un responsable especialista en seguridad general y otro de seguridad de la información.

El Control. Los controles pueden ser de dos tipos: control visual, que permiten eliminar muchos riesgos de forma sencilla, y los controles de validez, que se basan en estadísticas para indicar o avisar de posibles riesgos inminentes y así poder prevenirlos. Estos controles sólo podrán realizarse si existen reglas definidas, recogidas normalmente en forma de reglamentos de régimen interior, que deberán ser mantenidos diariamente y debidamente actualizados. Estas normas deben estructurarse por función, por proceso, por operación, por tipo de información y por sección o importancia del riesgo.

La Auditoría. Se debería tener definida la función de Auditoría Interna con la misión de efectuar periódicamente revisiones para comprobar el grado de cumplimiento de la normativa interna, participando activamente en la definición de los nuevos sistemas de información para dotarles de las medidas de seguridad necesarias y de los elementos que faciliten su auditabilidad. En aquellas organizaciones que por su reducido tamaño no sea aconsejable tener esta función, sería conveniente contratar periódicamente una empresa que realice la Auditoría para supervisar el estado de la seguridad informática.

4.3.2 El Entorno Físico

Los Edificios. Es necesario conocer el entorno circundante de los edificios donde está ubicada la Organización, para así poder prevenir los riesgos de seguridad. Se deberían implantar controles de acceso, sistemas antiparásitos en las redes eléctricas, sistemas de detección de incendios, sistemas de vigilancia y observación.

Las Salas de Cómputo. Según el equipo a proteger, se requeriría de unas medidas de seguridad u otras. Todo depende de lo crítico de la información y de su sensibilidad a ser utilizada de forma delictiva. También es necesario asegurar la gestión de la continuidad del negocio, por lo que es necesario dotar las salas de sistemas de alimentación ininterrumpida (SAI o UPS). En cuanto al material magnético de almacenamiento y copias de seguridad, se deberían almacenar en armarios antiincendio y en salas separadas, ya sea al interior de la organización o contratar una empresa que se encargue de este tipo de almacenamientos informáticos.

4.3.3 El Entorno Lógico

Se deben tener en cuenta las políticas y normas de seguridad, los procedimientos de revisión, los medios de emergencia, los medios de controles programados, la seguridad general, los sistemas de información y telecomunicaciones. Se debe considerar:

- Identificación y evaluación de los riesgos.
- Definición de los riesgos intolerables y jerarquización de las necesidades.
- Medios de tratamiento de los riesgos, tanto de prevención como de mitigación y resolución, en caso de que aparezcan.
- Estudio de las vulnerabilidades de la organización y del entorno, y medidas para corregirlas.

Además, se debe saber cuáles son las fallas más comunes que puedan dar lugar a la falta de seguridad y que, por lo tanto, deberían cuidarse con especial atención:

- **Cifrado**. Aunque los sistemas de cifrado son una herramienta que aumenta la seguridad de las comunicaciones, hay que tener en cuenta que estos pueden causar problemas al ocultar virus a los antivirus perimetrales que no estén preparados para ellos. La única solución para evitar que los virus cifrados entren en la empresa debe ser una protección perimétrica efectiva que bloquee los elementos cifrados no autorizados antes de que puedan alcanzar los servidores y las estaciones de trabajo de la empresa.

- **Sistema de Seguridad**. Son los procedimientos que se establecen para garantizar que el sistema es seguro, está bien planteado y definido.

- **Confianza.** Se piensa que el sistema funcionará siempre bien y no se llevan a cabo ciertas verificaciones necesarias para la prevención de problemas. Además, se puede pensar que la información que se tiene no es de interés para terceros, o que nunca se van a tener ataques por parte de terceros, y se descuidan las medidas de seguridad y prevención.

- **Desconexión de Línea.** Muchos sistemas toleran una desconexión de una línea sin dar por finalizada la sesión del usuario que está conectado, de manera que al restablecerse la conexión, podría otro usuario continuar con la sesión accediendo a la información del que realmente está dado de alta. Esta situación se debería evitar, dando por finalizada la sesión del usuario, el cual podrá comenzarla de nuevo cuando se recupere la conexión.

- **Sistema de Contraseñas.** Las contraseñas son fáciles de obtener o deducir. Sería preferible, sobre todo en los sistemas actuales basados en la transmisión de datos, utilizar certificados seguros para identificar a los usuarios.

- **Trampas Indebidas**. Muchos sistemas ofrecen diversas trampas con el fin de atraer a los intrusos inexpertos y así conducirles hacia puntos en que no pueden hacer nada. Si dichas trampas no funcionan correctamente pueden ser una buena forma de transgredir la seguridad del sistema que es precisamente lo que tratan de evitar. Algunas de estas trampas son los *Honeypots* y los *Honeynets*.

- **Privilegios.** Hay sistemas que admiten gran cantidad de privilegios para los usuarios y programas; si existe algún programa con muchos de estos privilegios, puede representar una futura penetración al sistema. A los programas sólo se les deberán conceder los privilegios que sean realmente imprescindibles.

- **Malware (Virus, Caballos de Troya, Gusano o Bomba Lógica)**. Desactualización del software que controla y destruyan estos tipos de programas maliciosos.

- **Prohibiciones**. Se impide a los usuarios el acceso a determinadas zonas o recursos del sistema, pero los mecanismos dispuestos no son perfectos, o no se han implantado adecuadamente y los usuarios pueden acceder fácilmente a los mismos.

- **Basura.** Lo que puede parecer impensable en la mayoría de los casos es la principal fuente de información para los intrusos. Se debe tener en cuenta que los residuos y papeles depositados en una papelera pueden ofrecer mucha información a posibles usuarios desalmados.

- I**ntentos de Acceso.** El sistema deberá tener un conteo con el número de intentos de entrada fallidos que realiza un usuario, y a partir de una cierta cantidad de ellos, dicho usuario deberá ser bloqueado, impidiéndole el establecimiento de cualquier sesión, ya que si no se bloquean estos usuarios, en algún momento podrán ingresar, creando un hueco en la seguridad de la información de la empresa.

4.4 AUTENTICACIÓN

Se emplean sistemas de autenticación en la mayoría de las actividades diarias de las organizaciones. En las transacciones relacionadas con información personal o financiera, se debe mostrar una prueba de identidad. La autenticación puede tomarse en dos contextos diferentes:

4.4.1 Autenticación de Usuario

La autenticación de usuario busca determinar si el usuario es quien dice ser. Es decir, lo que quiere es garantizar, por ejemplo, que si el usuario dice ser “X” es realmente “X”.

4.4.2 Autenticación de Datos

La autenticación de datos garantiza que el mensaje enviado es realmente el mismo que el mensaje recibido. Aquí, lo importante no es mantener la confidencialidad de los datos, sino garantizar que no se ha alterado el mensaje durante la transmisión. Para la autenticación de datos, se codifica un mensaje utilizando una clave de encriptación, transmitiendo tanto el mensaje codificado como el no codificado al interlocutor. A la recepción de los mensajes, el interlocutor utiliza la clave de encriptación para descodificar el mensaje codificado, comparándolo con el mensaje original no codificado. Si coinciden los dos mensajes, el destinatario puede estar seguro que no se alteró el mensaje durante la transmisión.

4.5 NO REPUDIO

Cuando se recibe un mensaje, no sólo es necesario poder identificar de forma unívoca al remitente, sino que éste asuma todas las responsabilidades derivadas de la información que envía. En este sentido, es fundamental impedir que el emisor pueda rechazar o repudiar un mensaje, es decir, negar su autoría sobre la información que envía y sus posibles consecuencias. A esto se denomina no repudio en el contexto de la transmisión de datos.

4.6 TRAZABILIDAD

Es la capacidad para reconstruir el historial de la utilización o la localización de alguna información o sistema, mediante una identificación registrada. Un proceso de trazabilidad completo y fiable es una de las herramientas indispensables a la hora de prevenir y detectar una crisis cuando las políticas y los controles de seguridad no son efectivos.

4.7 RESPONSABILIDAD

Es la propiedad de una entidad que garantiza que las acciones de ésta, como violación o intento de violación de la seguridad, queden asociadas inequívocamente a ella.

4.8 SEGURIDAD TOTAL

No importa cuántos controles, claves o seguros se utilicen, NUNCA se tendrá "Seguridad Total". Cuando se establecen políticas y actividades para administrar la seguridad de una red, lo que se busca es reducir la probabilidad de ocurrencia de fallas o daños en proporción a las medidas de protección tomadas. El grado de protección necesaria está basado en el valor de la información y de los procesos que se desean proteger: para la información y los procesos más importantes se deben destinar más recursos.

5. MEJORES PRÁCTICAS Y NORMAS DE SEGURIDAD

En este apartado se hablará acerca de los modelos, normas y prácticas de seguridad más difundidas en nuestro medio y que darán apoyo al modelo de seguridad propuesto.

5.1 ESQUEMA DE COBIT

CoBiT fue desarrollado y es mantenido por el *IT Governance Institute* (ITGI) desde 1998 con el fin de crear estándares internacionales para la gobernabilidad TI en las empresas. Es un marco de referencia que ayuda a satisfacer las múltiples necesidades de la administración de la organización estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Las "buenas prácticas" de CoBiT – que reúne el consenso de expertos- ayudarán a optimizar la inversión de la información a través de un dominio y un marco referencial de los procesos, y proporcionarán un mecanismo de medición que permitirá juzgar cuando las actividades van por el camino equivocado.[4]

"CoBit está diseñado para ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de los riesgos, así como de los beneficios asociados con la información y sus tecnologías relacionadas."[5]

Los resultados que se esperan encontrar con la implementación de Cobit dentro de la organización sobre los recursos de TI, son: eficiencia, efectividad, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información, los cuales son los pilares fundamentales de la seguridad de la información.

El modelo Cobit reconoce la importancia que tiene la gerencia en la implementación y manejo del modelo dentro de la organización y por tal motivo asigna responsabilidades críticas a esta área, las cuales son:

---

[4] *e-stratega.com.ar/cobit.htm*
[5] *COBIT, Objetivos de Control, Tercera Edición, año 2000, Comité directivo de Cobit, IT Governance Institute, Página 7.*

- Asegurar que los sistemas de control interno estén funcionando correctamente y soportan los procesos de negocio.

- Además, debe garantizar que todas las personas involucradas en la administración, uso, diseño, desarrollo, mantenimiento u operación de los sistemas de información actúen con la debida diligencia.

El marco de referencia de Cobit consta de 34 objetivos de alto nivel, distribuidos en los siguientes cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega de Servicios y Soporte, y Monitoreo, con los cuales se busca cubrir todos los aspectos de información y tecnología que soportan la organización. El marco de referencia proporcionado por CoBit contiene una guía o directriz de Auditoría, que permite evaluar los objetivos de alto nivel, y de esta manera suministrar a la gerencia la información necesaria para conocer el estado actual de los procesos. Además, CoBit recomienda 318 objetivos de control, que sirven como referencia para comparar los objetivos de alto nivel.

CoBit esta diseñando como un modelo de madurez en donde se *definen factores críticos de éxito* que servirán como insumos para controlar y evaluar los procesos de TI por parte de la alta gerencia y el departamento de TI, y a su vez permiten comparar el estado actual de la seguridad de la información en la organización frente a los requerimientos de las mejores practicas. La medición de los procesos de TI se realiza a través de *indicadores claves del logro de objetivos,* los cuales sirven como mecanismos de medición para monitorear los procesos de TI respecto a los requerimientos del negocio, y los *indicadores claves de desempeño,* que sirven para medir la ejecución de los procesos de TI frente al objetivo que se está buscando.

Por lo anterior, y debido al amplio alcance que sugiere CoBit en la evaluación de la seguridad de la información, la estructuración y desarrollo de los procesos y a su reconocimiento a nivel mundial, se decidió alinear el modelo de madurez de la información en este esquema de seguridad.

PROCESOS DE TI DEFINIDOS DENTRO DE LOS CUATRO DOMINIOS DE COBIT

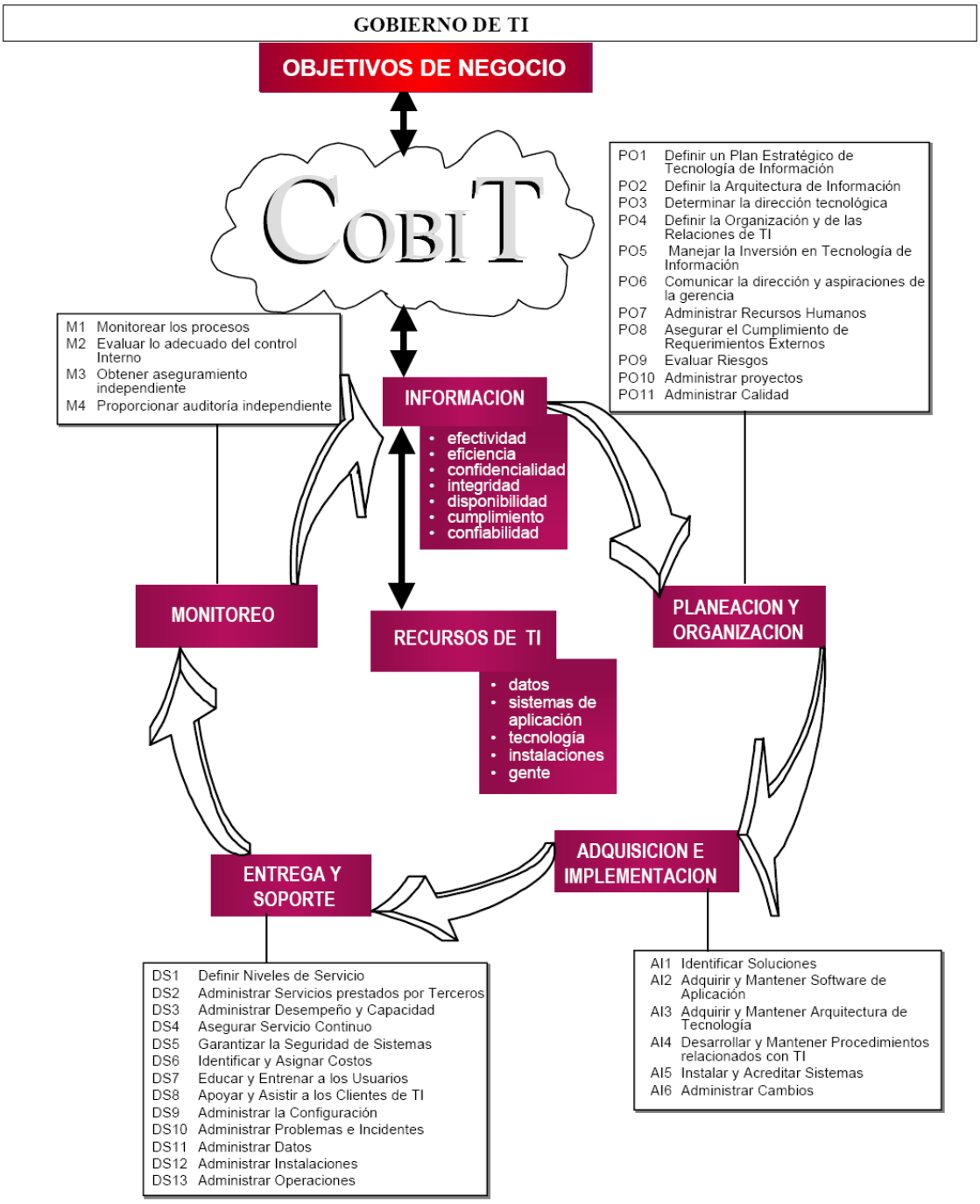

Figura 3. Modelo COBIT
Fuente: COBIT, Objetivos de Control

Actualmente se cuenta con la versión 4.0 de CoBit, la cual presenta mejoras significativas frente a la versión anterior, debido a su enfoque y lineamiento con normas internacionales como lo son ITIL, CMMI, COSO, PMBOK, ISF e ISO17799.[6] Además convierte el dominio de "Monitoreo" presente en la versión 3 en un dominio de "Monitoreo y Evaluación" en el cual se hace énfasis en las responsabilidades de TI.

Existen otros cambios significativos en la versión 4 de CoBit, sin embargo como el objetivo del modelo aquí propuesto no es la descripción detallada de CoBit, se sugiere al lector interesado en este tema comparar ambas versiones disponibles en el sitio Web de ISACA[7]

A pesar de que se reconoce las mejoras de esta nueva versión, el modelo aquí propuesto no utilizará esta actualización debido a que al momento de su publicación el modelo de madurez de seguridad de la información se encontraba en una etapa muy avanzada y soportado en la versión 3 de CoBit.

5.2 ESQUEMA NORMA ISO 17799

La ISO (*International Organization for Standardization*, por sus siglas en inglés) es una institución creada en 1947 la cual está diseñada por una red de instituciones de estandarización en 146 países, con una Secretaría General en Ginebra, Suiza y que trabaja en conjunto con organizaciones internacionales, gobiernos y representantes de industrias, empresas y representantes de los consumidores.

La norma ISO 17799 o anteriormente conocida como BS 7799 (*British Standard Institute*, 1999) y publicada por la ISO en diciembre de 2000, surgió debido a la necesidad que tenían las organizaciones de proteger la información y a la falta de un estándar o normativa que reuniera todos los aspectos a considerar por parte de las organizaciones, para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla.

[6] *http://es.sys-con.com/read*
[7] *http://www.isaca.org.*

Anteriormente las empresas consideraban que tenían que protegerse de los incidentes externo, pero con el paso del tiempo se percataron de que no sólo existían este tipo de amenazas sino que también habían peligros dentro de las organizaciones, y todos éstos deberían ser contemplados a la hora de protegerse. La aparición de esta normativa de carácter internacional ha supuesto una buena guía para las empresas que pretenden mantener de forma segura sus activos.

La ISO 17799 es una guía de buenas prácticas de seguridad informática que presenta una extensa serie de controles de seguridad y que no sólo cubre la problemática de la TI (Tecnología de Información) sino que hace una aproximación holística a la seguridad de la información abarcando todas las funcionalidades de una organización, previniendo de esta manera accesos no autorizados, brechas en seguridad y garantizando la puesta en marcha de los sistemas después de algún inconveniente[8].

Esta norma se estructura en 10 dominios, en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización, divididos en tres aspectos que puede suponer un incidente en las actividades de negocio de la organización (Figura 4):

- Políticas de seguridad.
- Seguridad Organizacional.
- Clasificación y control de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de la continuidad del negocio.
- Conformidad legal.
- Gestión de incidentes de la seguridad de la información.

[8] *http://www.unixmexico.org/modules.php?name=News&file=article&sid=1148*

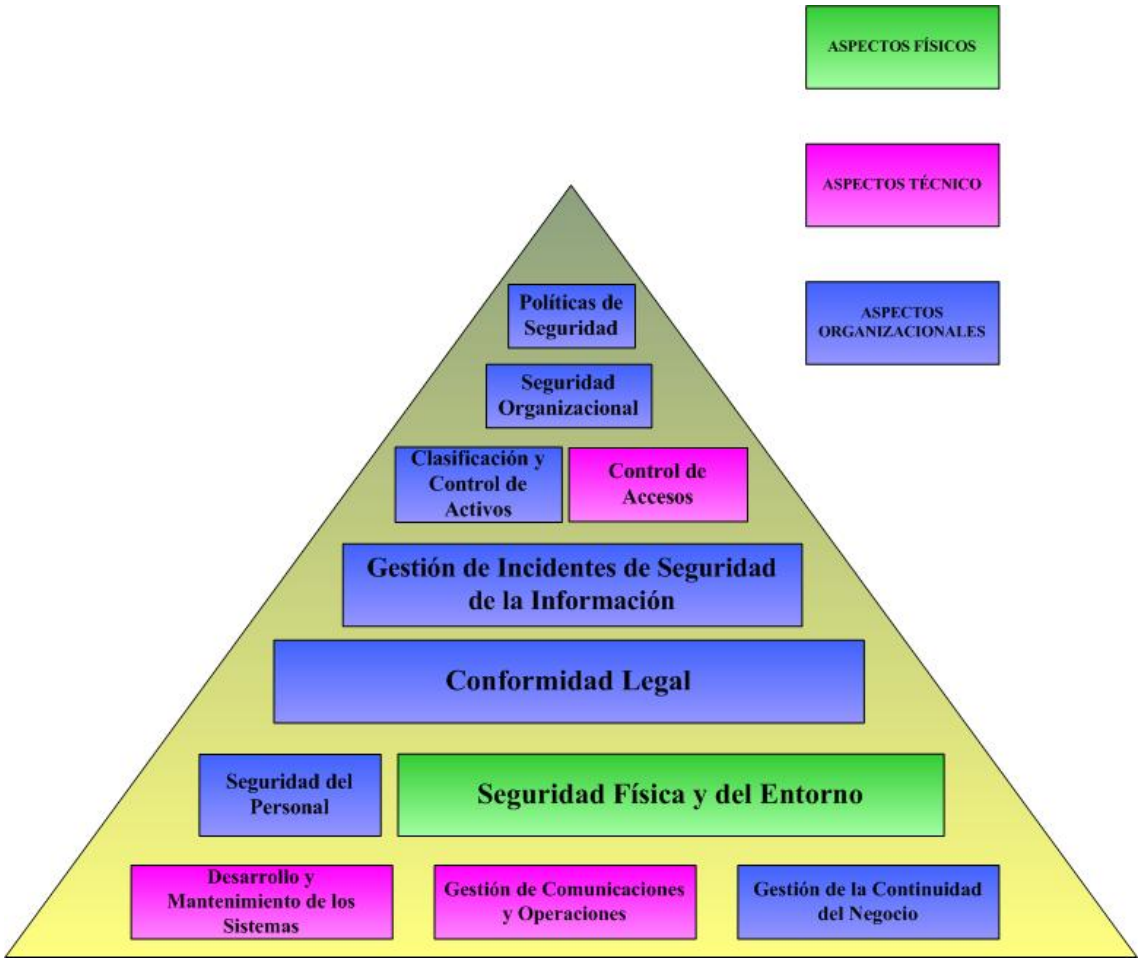

Figura 4. Modelo ISO 17799
Fuente: Adaptado de Organización DN-Systems[9]

Esta norma es aplicable a cualquier empresa, sea cual sea el tamaño, la actividad de negocio o el volumen del mismo, esto es lo que se denomina el principio de proporcionalidad de la norma, es decir, que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización. De la misma forma, dos organizaciones que tengan actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos/información. En pocas palabras, esta norma debe establecerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser implementados con los últimos avances, eso dependerá de la naturaleza de la propia organización.

[9] *www.dn-systems.de/Policy/BS7799/*

Actualmente se viene desarrollando la serie 27000, (correspondiente a la ISO 27000, 27001, 27002, 27003, 27004, 27005 y 270006) la cual será publicada a mediados del 2007. La ISO/IEC 27002 será una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información, la cual no será certificable y reemplazará la ISO17799:2005[10]. A continuación se describe cada uno componentes de esta serie[11]:

- ISO 27000: Esta en fase de desarrollo y contendrá todos los términos y definiciones que se emplean en la serie.

- ISO 27001: Es la norma principal de requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) en donde se enumera objetivos de control y controles que se sugieren implementar en el SGSI.

- ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Será la sustituta de ISO17799:2005, que es la que actualmente está en vigor, y que contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

- ISO 27003: Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA (Planear, Hacer, Revisar, Actuar) y de los requerimientos de sus diferentes fases.

- ISO 27004: Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Se enfocara en las fases de "Hacer" del ciclo PDCA propuesto en la ISO 27003.

- ISO 27005: Consistirá en una guía para la gestión del riesgo de la seguridad de la información.

- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

[10,11] *http://www.iso27000.es/*

5.3 ESQUEMA DE ITIL

ITIL (Biblioteca de infraestructura de Tecnología de información, por sus siglas en español) es un marco de trabajo de las mejores prácticas desarrollado para facilitar la entrega de servicios de TI de alta calidad.

Su desarrollo se remonta a la década de los 80´s cuando el gobierno británico a través de la CCTA (Agencia Central de telecomunicaciones y Cómputo) evidenció la necesidad de crear unas prácticas que permitieran estandarizar las operaciones de control y gestión de TI y evitar la proliferación de prácticas independientes desarrolladas por el sector privado y estatal.

A pesar que una organización no pueda certificarse en ITIL, su implementación le permite conocer el estado de su sistema de gestión de servicios de TI y servirá como base para obtener la certificación de la norma ISO/IEC 20000.

La estructura de ITIL esta desarrollada por un conjunto de libros, donde cada uno de ellos especifica una práctica dentro de la gestión de TI. Para la versión 2, se cuenta con 8 libros los cuales son:

- Entrega de Servicios
- Soporte al Servicio
- Gestión de la infraestructura de TI
- Gestión de la seguridad
- Perspectiva de negocio
- Gestión de aplicaciones
- Gestión de activos de software.
- Planeando implementar la Gestión de Servicios.

Una de las principales características de esta versión fue la agrupación de los 30 libros que contenía la versión anterior en estos 8 libros según los procesos de administración que cada uno cubría.

Fuera de eso, ITIL cuenta con un libro llamado "*ITIL Small Scale Implementation*" (Implementación de ITIL a Pequeña Escala), el cual es una guía con recomendaciones para departamentos de TIC pequeños.

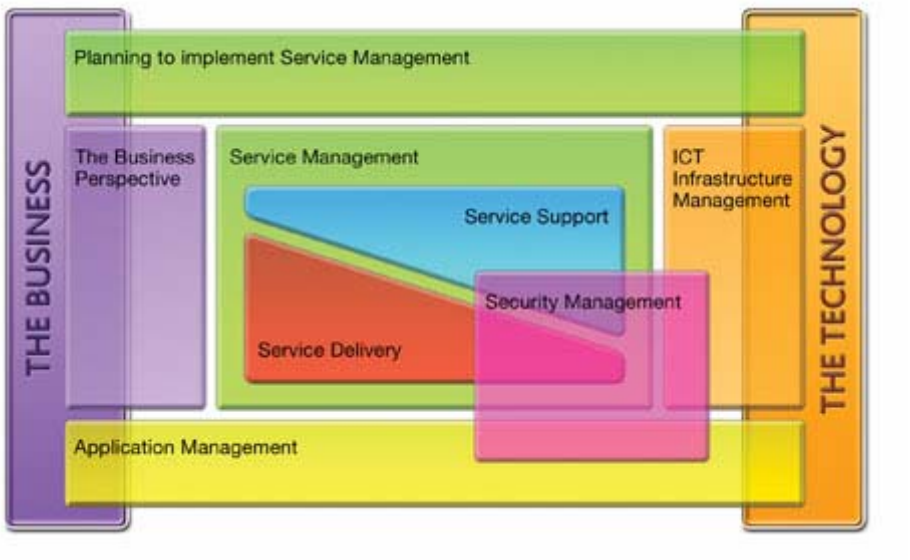

Figura 5. Esquema ITIL
Fuente: CASEWISE [12]

[12] *www.casewise.com/products/bpc-accelerator/1.php*

6 METODOLOGÍA DE TRABAJO DEL MODELO DE MADUREZ.

La estructura central del trabajo está soportado principalmente en la norma ISO 17799:2005, en el modelo CoBit versión 3 y en el trabajo de grado *"Hacia un modelo de Madurez para la Seguridad de la Información"*[13], en donde se plantea un modelo de seguridad basado en el modelo CMMI, que se utiliza actualmente para el desarrollo de software, y se establecen metas que relacionan este modelo con la norma ISO 17799.

El propósito principal del modelo que se está desarrollando actualmente es proporcionar a las organizaciones en general y/o a las empresas de consultaría una herramienta que permita evaluar el estado actual de la seguridad de la información, y a partir de estos resultados tomar medidas para corregir las debilidades encontradas y llegar al nivel óptimo que se desea. Para esto, el modelo que aquí se propone, está divido por niveles, en donde, para alcanzar un nivel superior, la organización deberá cumplir las metas que se diseñaron para el mismo. La importancia que tiene esta distribución por niveles es que la organización tendrá no solo una valoración cualitativa (reflejada en una posición en los diferentes niveles del modelo), sino que a su vez podrá identificar cómo ha sido la evolución de maduración de sus procesos. Esta descripción de los niveles y procesos se explican en los próximos apartados.

6.1 NIVELES DEL MODELO DE MADUREZ

El modelo que se plantea en este proyecto de grado está conformado, a diferencia del modelo CMMI, por seis niveles, los cuales son: Básico, Inicial, Gestionado, Definido, Gestionado Cuantitativamente y En Optimización. Se decidió adicionar el nivel Básico a este modelo, debido a que las empresas interesadas en utilizarlo deben cumplir con unos requisitos mínimos, como lo son la buena disposición de los empleados y la alta gerencia para el desarrollo del modelo, los recursos financieros destinados para el

[13] *Barrientos A. Andrea Marcela, Aleiza C. Karen Alexandra,INTEGRACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON UN SISTEMA DE GESTIÓN DE LA CALIDAD, Proyecto de Grado, Universidad EAFIT, 2005.*

desarrollo de la valoración, entre otros aspectos, que se presentarán en la descripción del nivel.

A su vez, cada uno de los niveles está conformado por Procesos, los cuales están definidos por el modelo CoBit, de los que se desprenden las metas que se deben cumplir para evaluar dichos procesos, y como consecuencia, el nivel que se pretende cumplir. La evaluación de estas metas se hace a través de criterios, los cuales fueron diseñados con base en los propuestos por la herramienta COBRA desarrollada por la empresa *C&A Systems Security Ltd*[14], la cual está soportada sobre la norma ISO 17799. En la figura 5 se presenta la organización del modelo propuesto.

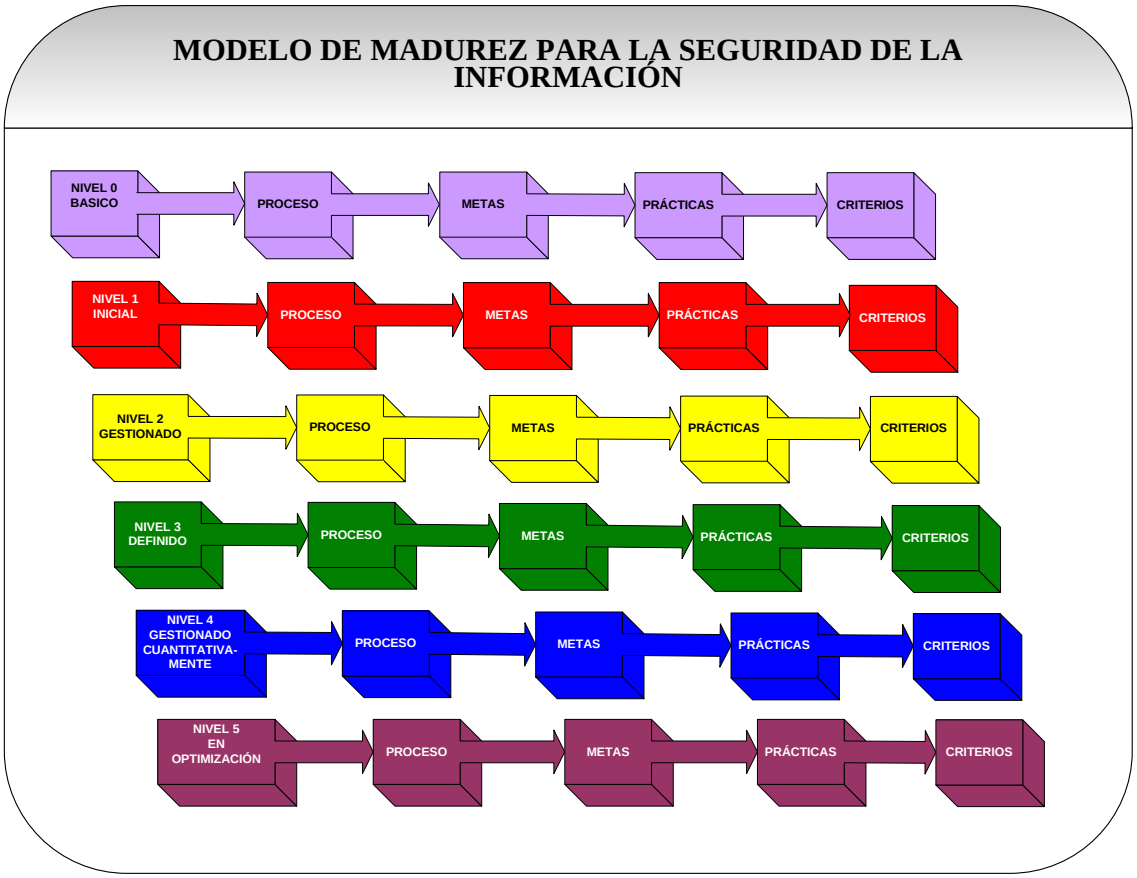

Figura 6. Modelo de Madurez Propuesto
Fuente: Elaboración propia.

A continuación se presenta cada uno de los niveles propuestos para el modelo de madurez y la descripción de cada uno de los procesos que lo conforman:

[14] *www.riskworld.net/*

6.1.1 Nivel 0 (Básico)

Objetivos.

- Disponer de los recursos financieros y humanos para el desarrollo del modelo de seguridad de la información dentro de la organización, y contar con canales de comunicación establecidos dentro de la organización para difundir la información.

- Tener establecidos y documentados los procesos de negocio de la organización.

Para este nivel no se desarrollaron procesos ya que lo que se busca es contar con un ambiente propicio para la implementación del modelo y en esta instancia aún no se ha iniciado la evaluación como tal.

6.1.2 Nivel 1 (Inicial)

Objetivo.

- Inventariar los recursos de tecnología, activos tangibles e intangibles con los que se cuenta en la actualidad y clasificarlos según su criticidad e impacto en el negocio y los riesgos a los que están expuestos. Así mismo, se debe iniciar una campaña de capacitación en seguridad de la información para todas las instancias de la compañía.

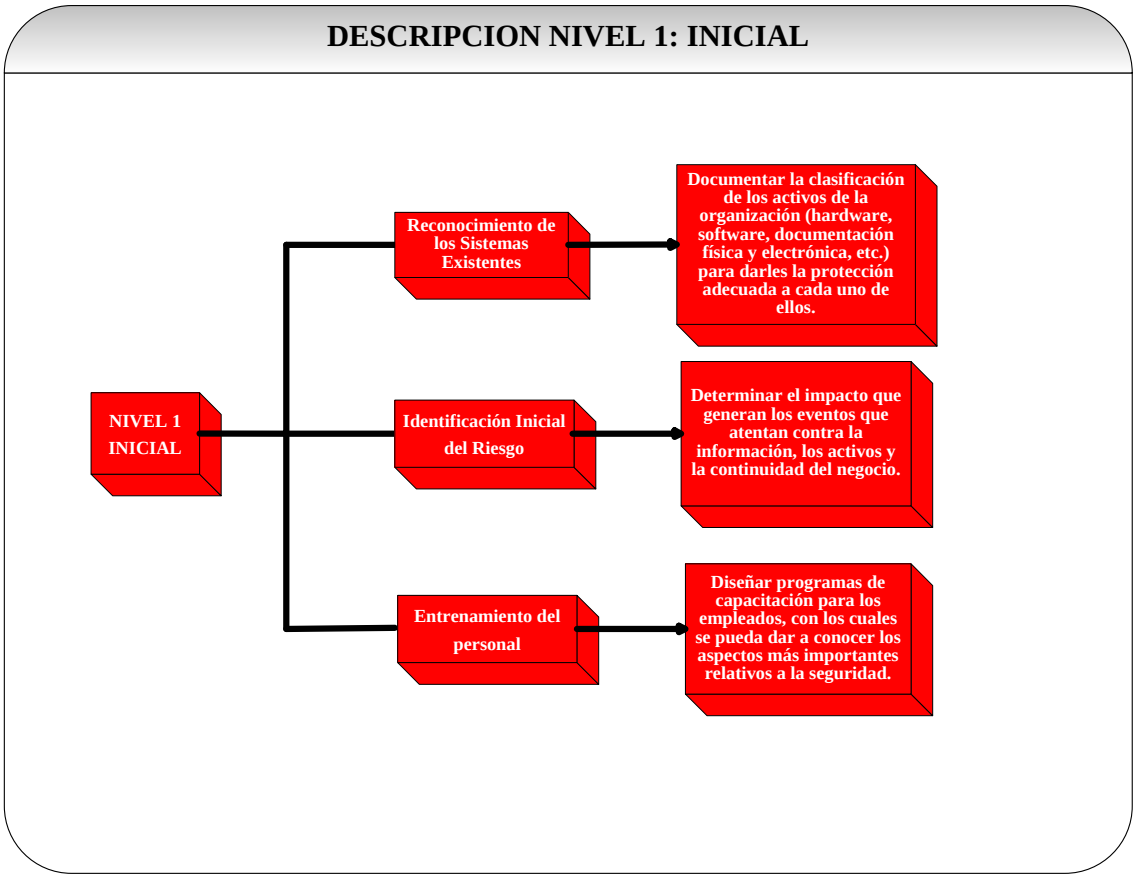

Figura 7: Nivel 1 Inicial
Fuente: Elaboración propia

Reconocimiento de los Sistemas Existentes

La gerencia de TI debe evaluar los sistemas existentes en términos de: nivel de seguridad, nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo, fortalezas y debilidades, con el propósito de determinar el nivel de soporte que ofrecen los sistemas existentes a los requerimientos del negocio.

Identificación del Riesgo

La evaluación de riesgos deberá enfocarse al exámen de los elementos esenciales de riesgo y las relaciones causa/efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, valor de los activos, amenazas, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. El proceso de identificación de riesgos debe incluir una clasificación cualitativa y, donde sea

apropiado, clasificación cuantitativa de riesgos y debe obtener insumos de las tormentas de ideas de la gerencia, de planeación estratégica, auditorías anteriores y otros análisis. El análisis de riesgos debe considerar el negocio, regulaciones, aspectos legales, tecnología, comercio entre socios y riesgos del recurso humano.

Entrenamiento del personal

La gerencia deberá implementar procesos para capacitar al personal de la organización en aspectos tanto de seguridad como técnicos; estos procesos deben estar en línea con las políticas y procedimientos generales de la organización. La administración debe asegurar que el conocimiento y las habilidades necesarias sean continuamente evaluados y que la organización esté en la capacidad de obtener una fuerza de trabajo que tenga las habilidades para satisfacer los objetivos y metas de la organización.

Además, la gerencia de la función de servicios de información deberá verificar regularmente que el personal que lleva a cabo tareas específicas esté calificado, tomando como base una educación, entrenamiento y/o experiencia apropiados, según se requiera. La gerencia deberá alentar al personal para que participe como miembro, en organizaciones profesionales.

6.1.3 Nivel 2 (Gestionado)

Objetivo.

- Diseñar, desarrollar y comunicar las intenciones y aspiraciones de la alta gerencia respecto a las políticas de seguridad que se implementarán en la organización. A su vez, se deben implementar sistemas de administración de problemas e incidentes que garanticen el normal funcionamiento de los procesos críticos de la organización, con base en la clasificación de los recursos tangibles e intangibles existentes.

Figura 8: Nivel 2 Gestionado
Fuente: Elaboración propia.

Implementar y mantener las políticas de seguridad y garantizar la aprobación y apoyo por parte de la gerencia.

La gerencia deberá asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cubran metas y directrices generales. Deberán llevarse a cabo revisiones regulares de las políticas para asegurar su conveniencia. La complejidad de las políticas y los procedimientos escritos deberán estar siempre en proporción con el tamaño de la organización y el estilo gerencial.

Comunicación de las intenciones y aspiraciones de la gerencia.

La gerencia deberá asegurar que las políticas organizacionales y el programa de concientización sobre seguridad de TI sean claramente comunicados, comprendidos y

aceptados por todos los niveles de la organización. El proceso de comunicación debe estar soportado por un plan efectivo que utilice diversos mecanismos de comunicación.

Creación del grupo interdisciplinario y relaciones con usuarios de TI.

La alta gerencia de la organización deberá designar un comité de planeación o dirección para vigilar la función de TI y sus actividades, así como llevar a cabo las acciones necesarias para establecer y mantener una coordinación, comunicación y un enlace óptimos entre los miembros del comité (representantes de la alta gerencia), la gerencia de TI y demás interesados, dentro y fuera de la función de servicios de información (usuarios, proveedores, oficiales de seguridad, administradores de riesgos). El comité deberá reunirse regularmente y reportar a la alta gerencia.

Evaluación y mantenimiento de los sistemas y datos existentes.

La gerencia deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de activos físicos y lógicos identificadas, con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de controles apropiados (mínimos) para cada una de las clasificaciones, así como la asignación de propiedad, y deberán ser reevaluados periódicamente y modificados en consecuencia.

Administración de problemas e incidentes.

La gerencia de TI deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos que impidan la normal operación del negocio (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Los procedimientos de cambios de emergencia a programas se deben probar, documentar, aprobar y reportar prontamente. Deberán emitirse reportes de incidentes en caso de problemas significativos.

Definición del plan de continuidad de TI

La gerencia de TI, en cooperación con los propietarios de los procesos del negocio, deberá crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque/metodología basada en riesgo a seguir y las reglas y la estructura para documentar el plan de continuidad de TI, así como los procedimientos de aprobación. Este plan debe tener consistencia con el plan general de continuidad de la empresa.

6.1.4 Nivel 3 (Definido)

Objetivos.

- Diseñar actividades que maximicen y motiven las contribuciones y el desarrollo de habilidades de los empleados de la organización, así como constantes capacitaciones y entrenamientos en temas de seguridad de la información y políticas de seguridad y la responsabilidad de cada empleado en el cumplimiento de está última.

- Implementar controles y sistemas de medición, que garanticen la seguridad en la organización y mitiguen al máximo los riesgos a los que está expuesta, basándose en el análisis costo-beneficio y que permitan monitorear su comportamiento a través de indicadores y *logs* de auditoría.

Figura 9: Nivel 3 Definido
Fuente: Elaboración propia.

Administración del Recurso Humano

Adquirir y mantener una fuerza de trabajo motivada y competente, y maximizar las contribuciones del personal a los procesos de TI a través de: prácticas de administración de personal, sensata, justa y transparente, para reclutar, alinear, compensar, entrenar, promover y despedir. Además, todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas, incluyendo actualizaciones periódicas con especial atención en concientización sobre seguridad y manejo de incidentes. La alta gerencia deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de TI, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.

Asignación de responsabilidades sobre la seguridad lógica y física

La gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un gerente de seguridad de la información, quien reportará a la alta gerencia. Como mínimo, la responsabilidad de la gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la misma. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos, con el fin de resolver los problemas de seguridad relacionados con ellos.

Implementación de controles e indicadores de medición.

Se deben establecer medidas que salvaguarden la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida, a través de controles de acceso lógico que aseguren que el uso de los sistemas, datos y programas está restringido a usuarios autorizados, teniendo en cuenta requerimientos de privacidad y confidencialidad, autorización, autenticación y control de acceso, identificación de usuarios y perfiles autorizados, las necesidades de los usuarios, prevención y detección de virus, y *firewalls*. De igual manera, se deben implementar indicadores de medición que permitan, en un futuro, el monitoreo de los controles implementados para la mitigación de los riesgos identificados contra la seguridad de la información en la organización.

Seguimiento de problemas y *logs* de Auditoría.

El sistema de administración de problemas deberá proporcionar adecuadas pistas de auditoría que permitan el seguimiento de un incidente a partir de sus causas (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

Administración de Instalaciones.

Las instalaciones donde se procesa información deben estar bajo un ambiente físico conveniente que proteja los equipos y al personal de TI contra peligros naturales o fallas humanas. Esto es posible a través de la instalación de controles físicos y ambientales adecuados, que sean revisados regularmente para garantizar su adecuado funcionamiento, teniendo en cuenta ciertos aspectos tales como: el acceso a instalaciones, la identificación del sitio (instalación), seguridad física, políticas de inspección y escalamiento, plan de continuidad de negocios y administración de crisis, salud y seguridad del personal, políticas de mantenimiento preventivo, protección contra amenazas ambientales y monitoreo automatizado.

6.1.5 Nivel 4 (Gestionado Cuantitativamente)

Objetivos.

- Mantener actualizado el plan de continuidad a través de pruebas y simulacros que permitan determinar su eficacia, y garantizar su correcto funcionamiento en caso de un evento de contingencia. Así mismo se debe realizar un monitoreo de los accesos y perfiles de cuentas de los usuarios propios de la empresa y de *outsourcing* que presten servicios en ella.

- Implementar actividades de monitoreo y seguimiento al cumplimiento de los objetivos de control interno a través de indicadores de desempeño gerenciales.

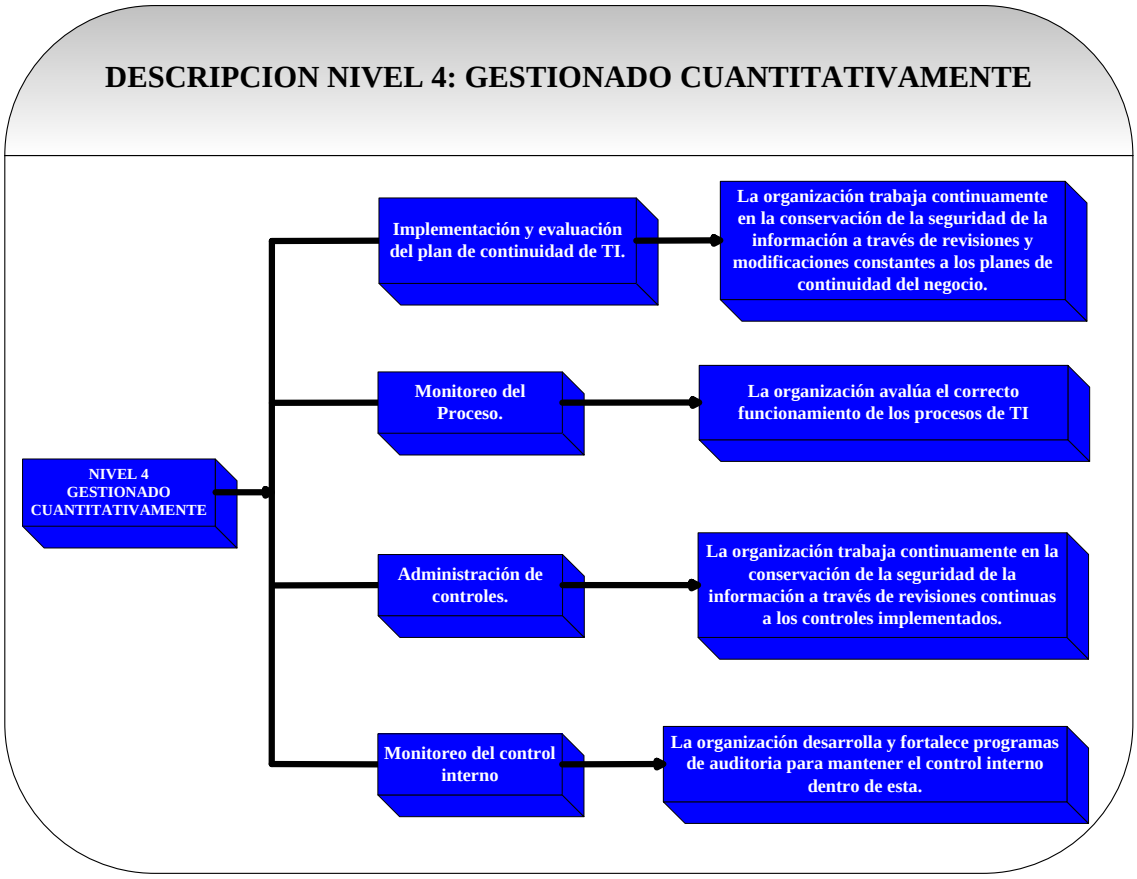

Figura 10: Nivel 4 Gestionado Cuantitativamente
Fuente: Elaboración propia.

Implementación y evaluación del plan de continuidad de TI.

Para contar con un plan efectivo de continuidad se debe distribuir la información de naturaleza sensitiva solo al personal autorizado, entrenar continuamente al personal sobre los procedimientos a ser seguidos en caso de un incidente o un desastre, garantizando a su vez procedimientos alternativos de los recursos críticos de tecnología de información y el tiempo máximo que estos pueden permanecer fuera de servicio hasta que se restablezca la normal operación. Además, se debe contar con sitios externos donde se almacenen copias de respaldo, documentación y otros recursos tecnológicos catalogados como críticos en los niveles anteriores.

Administración de controles.

La gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas

de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso. La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación. Los acuerdos de *outsourcing* deben considerar los riesgos, los controles sobre seguridad y los procedimientos para los sistemas de información y las redes en el contrato que se establece entre las partes. Además, se deben tener registros de la actividad de seguridad, garantizando que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente.

Monitoreo del proceso.

La gerencia debe asegurar el logro de los objetivos establecidos para los procesos de TI a través de los indicadores de desempeño gerenciales implementados en el nivel anterior y el reporte oportuno y sistemático del desempeño, desarrollando tarjetas de decisión (*scorecards*) con indicadores de desempeño y medición de resultados, evaluación de la satisfacción de clientes, creando una base de conocimientos del desempeño histórico y utilizando *Benchmarking* externo.

Monitoreo del Control Interno

La gerencia deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán generar análisis y acciones correctivas. Además, las desviaciones deberán ser comunicadas a la persona responsable de la función y también, por lo menos, a un nivel de la gerencia por encima de esa persona. Las desviaciones graves deberán ser reportadas a la alta gerencia.

6.1.6 Nivel 5 (En Optimización).

Objetivo.

- Alinear el plan de continuidad del negocio y los objetivos de control interno respecto a los cambios tecnológicos, administrativos y procedimientos de recursos humanos que se hayan dado, tanto dentro de la organización como en el entorno donde opera.

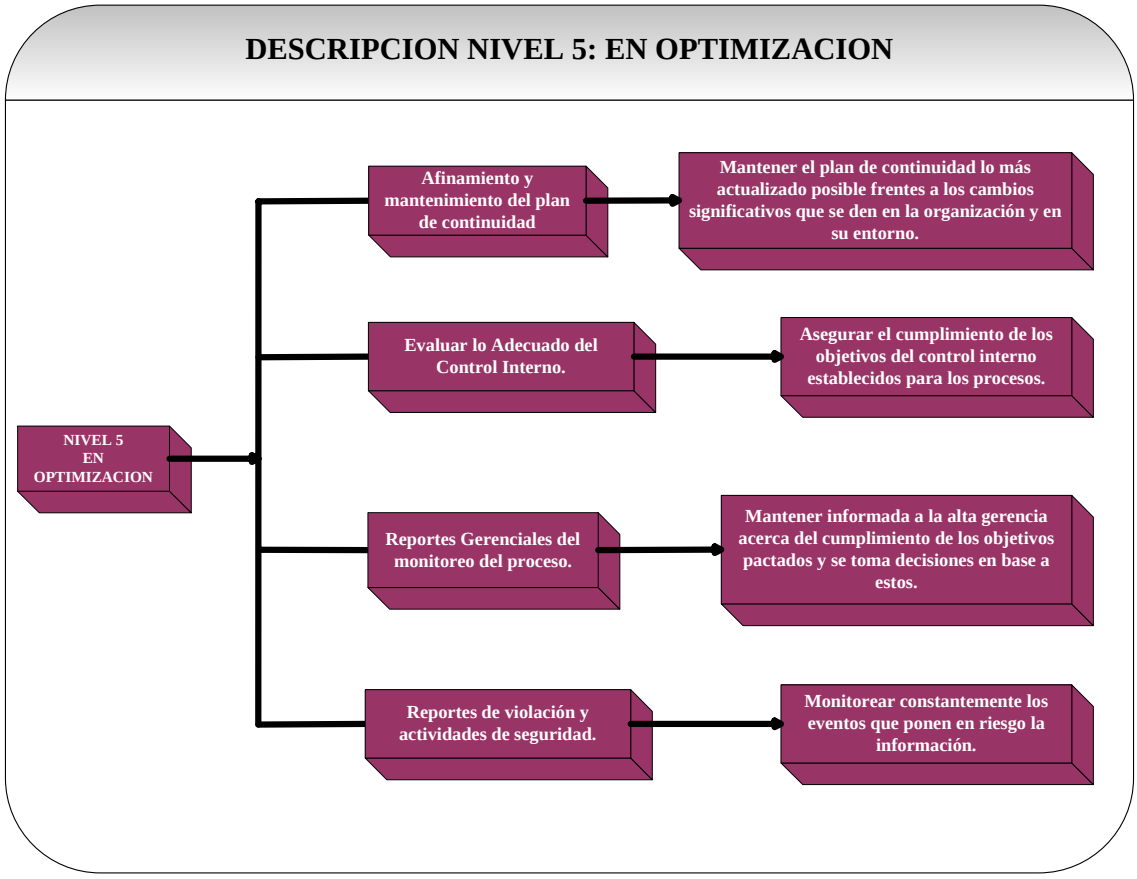

Figura 11: Nivel 5 En Optimización
Fuente: Elaboración propia.

Afinamiento y mantenimiento del plan de continuidad.

La gerencia de TI deberá proveer procedimientos de control de cambios para asegurar que el plan de continuidad se mantenga actualizado y refleje los requerimientos del negocio actual. Esto requiere de procedimientos de mantenimiento del plan de continuidad alineados con el cambio, la administración y los procedimientos de recursos humanos.

Reportes de violación y actividades de seguridad.

La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros *logs*) deberá otorgarse tomando como base el principio de menor privilegio o necesidad de saber.

Reportes Gerenciales del monitoreo del proceso

Deberán proporcionarse reportes gerenciales para ser revisados por la alta gerencia en cuanto al avance de la organización hacia las metas identificadas. Los reportes de estatus deberán incluir en qué medida se han logrado los objetivos planeados, se han obtenido productos, se han cumplido los objetivos de desempeño y se han mitigado los riesgos. Con base en la revisión, la gerencia deberá iniciar y controlar las acciones pertinentes.

Evaluar lo adecuado del control interno

La gerencia deberá reportar información sobre los niveles de control interno y sobre las excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno; además, la seguridad en las operaciones y el aseguramiento de control interno deberán ser establecidos y repetidos periódicamente a través de un "*autoanálisis*" o de una auditoria independiente.

6.2 MADUREZ DE LOS PROCESOS

Como lo propuesto en este proyecto de grado es un modelo de madurez, es de esperarse, que los procesos que lo conforman se fortalezcan y se incorporen cada vez más en la organización, debido al ascenso que realicen estos a través de los niveles que se proponen en el modelo.

Esta maduración de los procesos descrita en la figura 11, presenta la evolución que tienen los principales procesos en la seguridad de la información, resaltando la importancia que tiene la correcta identificación de los riegos, y la repercusión que tiene este proceso en el desarrollo de todos los otros; a su vez, se destaca la importancia que tiene la sinergia que debe existir entre los distintos departamentos de la organización, como lo son recursos humanos, gerencia directiva, usuarios y dueños de procesos organizacionales, entre otros, para lograr el éxitos de la evaluación del modelo y mitigar al máximo los riesgos a los que está expuesta la organización.

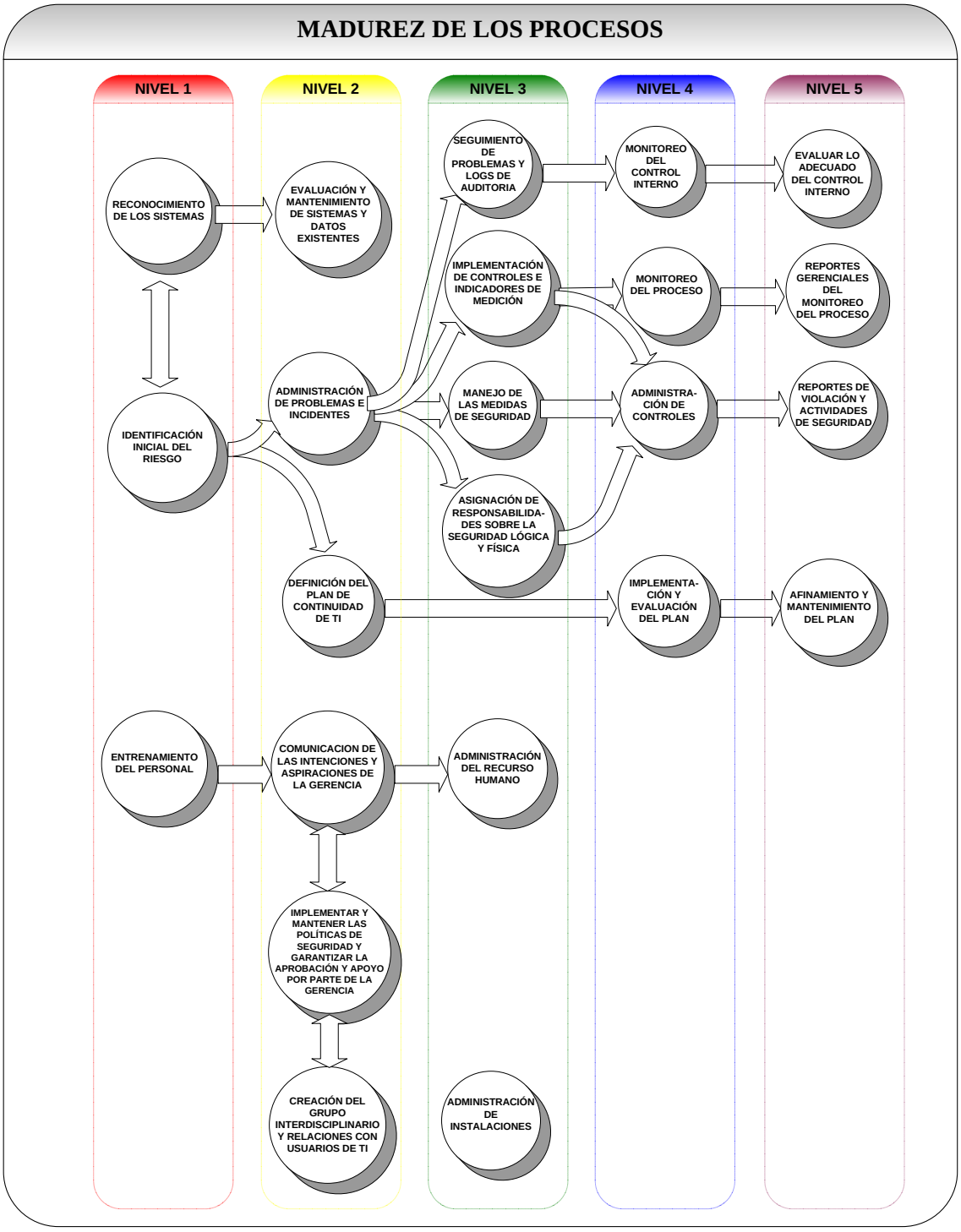

Figura 12: Madurez de los procesos
Fuente: Elaboración propia

En la figura 11 se describe como los procesos que se tienen definidos para el modelo de seguridad emprenden una etapa de maduración a medida que van avanzando entre los niveles establecidos, procurando que los procesos del modelo se integren a través del tiempo y de mejoras continuas a las actividades de negocio, iniciando con una etapa de reconocimiento de sistemas, identificación de riesgos a los que está expuesta la

organización y un entrenamiento básico del personal acerca de temas organizacionales y de seguridad de información, para posteriormente pasar a un nivel Gestionado donde se perfecciona la clasificación inicial de los sistemas y datos existentes, se establecen actividades para administrar incidentes y se inicia con la definición de un plan de continuidad del negocio a partir de los riesgos identificados en el nivel anterior, de igual forma se debe establecer y divulgar el plan de acción definido por la alta gerencia para controlar y garantizar la seguridad de la información y la conformación de un grupo interdisciplinario encargado de tratar temas de seguridad de la información y mantener constante comunicación con usuarios y la alta gerencia; luego de esto, para el nivel 3 se deben implementar controles e indicadores de medición que permitan en una etapa posterior conocer la efectividad de los controles implementados en esta instancia; se debe tener establecido el manejo de las medidas de seguridad y asignar responsabilidades sobre los activos físicos y lógicos que se establecieron en niveles anteriores. También es fundamental diseñar medidas que permitan que el personal se encuentre motivado y actualizado acerca de la implementación y manejo de la seguridad de la información que se inició en el nivel 1.

En nivel 4 del modelo de seguridad de la información se desarrollan procesos que permiten monitorear los controles implementados en el nivel anterior para mitigar los riesgos identificados, a su vez se busca evaluar que la organización ejecute y evalué el plan de continuidad del negocio diseñado en los niveles anteriores.

Para finalizar, el nivel 5 busca retroalimentar a la organización acerca de lecciones aprendidas sobre los incidentes y eventualidades que se han presentado, y establecer reportes del monitoreo de los procesos previamente implementados para tomar medidas y establecer planes de acción.

6.3 DEFINICIÓN DE CRITERIOS DE EVALUACIÓN.

Los criterios definidos para cada uno de los niveles que conforman el modelo de madurez fueron diseñados con el fin de permitir profundizar en los elementos más relevantes que se requieren evaluar en una organización, por tal motivo se realizó una ponderación de los criterios a partir de su importancia y relevancia en la evaluación de cada uno de los procesos.

Los criterios que se presentan en este modelo de madurez fueron diseñados a partir de los elementos de evaluación propuestos por la herramienta COBRA[15], la cual sirve para identificar fortalezas y debilidades frente a la seguridad de la información en base a la norma ISO 17799.

A pesar de que los criterios definidos para el modelo de madurez identifican los puntos críticos que se deben tener en cuenta para determinar el estado actual de la seguridad de la información en una organización, es necesario que las personas que los evalúen cuenten con conocimientos suficientes en sistemas de información, habilidades en la indagación y comunicación para obtener un mayor beneficio en el desarrollo del modelo de madurez en una organización.

[15] *www.riskworld.net/*

7 DEFINICIÓN DE LA METODOLOGÍA DE EVALUACIÓN

A continuación se presenta la metodología que servirá como guía de evaluación para el desarrollo del modelo que se definió anteriormente. Esta metodología es la relación que se estableció entre los procesos, metas, prácticas y criterios dentro de cada nivel que conforma el modelo de madurez propuesto.

7.1 NIVEL 0 (BÁSICO)

Como requerimientos mínimos para la implementación del modelo propuesto, la empresa interesada deberá cumplir por lo menos con los siguientes criterios:

- La alta gerencia está motivada para la implementación del modelo, esto es, que está dispuesta a apoyar con recursos necesarios tanto financieros como humanos.

- Los empleados se encuentran motivados y dispuestos a realizar dicha implementación, conocen el alcance y existen canales de comunicación establecidos dentro de la organización para difundir la información.

- Se tienen establecidos y documentados los procesos de negocio de la organización, sus responsables y una línea de autoridad definida.

Si la empresa cumple con todos los anteriores criterios, es posible dar comienzo a la implementación del modelo de madurez en la organización. En caso contrario, se recomienda no realizar dicha evaluación hasta que se fortalezcan estos puntos, debido a que se requiere garantizar la madurez de los procesos y del conocimiento del negocio de la organización, para garantizar una óptima implementación y los resultados del modelo.

7.2 NIVEL 1 (INICIAL)

En este nivel la organización no ha realizado ninguna evaluación de riesgo que permita ver las falencias que se tienen con relación a la seguridad de la información, por lo tanto, los controles existentes fueron desarrollados de manera informal y la seguridad es manejada a criterio de cada uno de los empleados, además no se toman medidas preventivas ante algún suceso.

Proceso:
Reconocimiento de los Sistemas Existentes:

Metas, criterios de evaluación y prácticas:

Meta: Documentar la clasificación de los activos de la organización (hardware, software, documentación física y electrónica, etc.) para darles la protección adecuada a cada uno de ellos.

Criterios de evaluación:

Práctica: Clasificación de activos físicos y lógicos.

¿Tienen los activos de la información alguna clasificación de Seguridad?

- Sí.
- No.

¿Existe algún esquema de clasificación de los activos lógicos y físicos de la organización y está debidamente documentado dicho esquema?

- Sí.
- No

¿Esta clasificación de los activos se basa en la funcionalidad, costos, soporte a los procesos críticos del negocio, fortaleza y debilidades de estos?

- Sí.
- No

Proceso:
Identificación inicial del riesgo.

Metas, criterios de evaluación y prácticas:

Meta: Determinar el impacto que generan los eventos que atentan contra la información, los activos y la continuidad del negocio.

Criterios de evaluación:

Práctica: Identificación inicial del riesgo.

¿El proceso que evalúa y determina los riesgos a que está expuesta la organización comienza identificando los acontecimientos que pueden causar interrupciones a los procesos del negocio e incluyen el costo del impacto de estas interrupciones?

- Sí.
- No.

¿El análisis de riesgo a los que está expuesta la organización tiene en cuenta los puntos de vista de la gerencia, la planeación estratégica, los resultados de las auditorías y los incidentes ocurridos?

- Sí.
- No.

Proceso:

Entrenamiento de personal

Metas, criterios de evaluación y prácticas:

Meta: Diseñar programas de capacitación para los empleados, con los cuales se pueda dar a conocer los aspectos más importantes relativos a la seguridad.

Criterios de evaluación:

Práctica: Capacitación en seguridad y entrenamiento técnico.

¿Todos los usuarios han recibido una adecuada capacitación de seguridad y entrenamiento técnico?

- Sí.
- No.

¿La capacitación y el entrenamiento incluyen políticas y procedimientos de la organización, así como el uso correcto de las instalaciones de procesamiento de información antes de que se conceda el acceso a dichas instalaciones?

- Sí.
- No.

¿Estas actividades de entrenamiento se ejecutan de forma periódica para garantizar el aprendizaje continuo?

- Sí.
- No.

7.3 NIVEL 2 (GESTIONADO)

Existen procesos básicos de gestión de la seguridad de la información. Los controles existentes hacen que se puedan detectar posibles incidentes de seguridad.

Proceso:
Implementar y mantener las políticas de seguridad y garantizar la aprobación y apoyo por parte de la Gerencia.

Metas, criterios de evaluación y prácticas:

Meta: Revisar y aprobar las Políticas de Seguridad de la información. Esta revisión debe ser hecha por los directivos de la organización.

Criterios de evaluación:

Práctica: Diseño de política de seguridad.

¿La política contiene una declaración de la intención de la gerencia que apoya las metas y los principios de la seguridad de la información?

- Sí.
- No.

¿La política contiene una definición de la seguridad de la información - sus objetivos y alcance totales - y de su importancia como mecanismo que permite administrar la información dentro de la organización?

- Sí.
- No.

¿La política contiene detalles de un marco de la seguridad (factores a evaluar), y un gravamen y programa de la gerencia de riesgo?

- Sí.
- No.

¿La política contiene una explicación de las reglas específicas de seguridad organizacional, los principios, los estándares y los requisitos de conformidad, de acuerdo con aspectos legislativos, políticas de la continuidad del negocio y consecuencias por violaciones?

- Sí.
- No.

Práctica: Revisión de la política de seguridad.

¿Hay un proceso de revisión definido, que incluye responsabilidades y fechas de revisión para mantener el documento de la política?

- Sí.
- Proceso *ad-hoc* solamente.
- No existe procesos de revisión.

¿La revisión de la política de seguridad incluye la evaluación de la eficacia de las políticas, el costo beneficio de los controles iniciales que se tienen y los cambios tecnológicos dados en la organización?

- Sí.
- No.

¿Quedan registrados los temas que se trataron en la revisión de la política de la seguridad en actas con las firmas de aprobación de la alta Gerencia para ser evaluadas en las próximas revisiones?

- Sí.
- No.

Práctica: Asignar responsable de administrar la política.

¿La política tiene un dueño claro, el cual ha aceptado su responsabilidad en la administración de ésta, y esta aprobación queda registrada en un acta?

- Sí.
- No.

Proceso:

Comunicación de las Intenciones y Aspiraciones de la Gerencia

Metas, criterios de evaluación y prácticas:

Meta: Elaborar un plan para divulgar las Políticas de Seguridad de la información de la organización.

Criterios de evaluación:

Práctica: Distribución de la política de seguridad al personal correspondiente.

¿Existe un documento escrito de políticas de la seguridad, conocido y disponible para TODO el personal en la organización responsable de la seguridad de la información?

- Sí.
- No

¿Se realizan actividades para aclarar dudas acerca de la política de seguridad comunicada a los empleados, para garantizar su comprensión?

- Sí.
- No

Proceso:

Creación del grupo interdisciplinario de seguridad y relaciones con usuarios de TI

Metas, criterios de evaluación y prácticas:

Meta: Establecer que las reuniones del grupo interdisciplinario sean lo más formal posible, es decir, se planeen y se dejen actas sobre los temas trabajados durante la reunión y sobre las acciones o compromisos pendientes, para el manejo de la información al interior de la organización.

Criterios de evaluación:

Práctica: Creación y definición de actividades del grupo interdisciplinario.

¿Existe dentro de la organización un foro de alto nivel (expertos en seguridad de la información internos y/o externos y representantes de la alta gerencia) para el manejo de la seguridad de la información para dar orientación y soporte a la administración?

- Sí.
- No.

¿Entre los temas tratados por el foro de seguridad de la información se tienen, la revisión de las políticas de la compañía, el monitoreo de las amenazas de los activos, la revisión de los incidentes ocurridos y las sanciones de estos, y las actividades de seguridad que se desarrollarán, entre otros?

- Sí.
- No.

Práctica: Creación del comité Inter-funcional y definición de sus actividades.

¿Existe un comité Inter-funcional para coordinar medidas de seguridad de la información?

- Sí.
- No.

¿Entre los temas que son tratos por el comité Inter-funcional está el de determinar los roles y responsabilidades dentro de la organización, las iniciativas que se llevarán a cabo dentro de la organización sobre temas de seguridad, la coordinación e implementación de las nuevas medidas de seguridad y la revisión de los incidentes?

- Sí.
- No.

Proceso:

Evaluación y mantenimiento de los sistemas y datos existentes

Metas, criterios de evaluación y prácticas:

Meta: Tener un inventario de los activos físicos y lógicos de la organización lo más completo posible.

Criterios de evaluación:

Práctica: Mantenimiento del inventario de los activos físicos y lógicos.

¿Existe mantenimiento al inventario de los activos de la organización?

- Sí.
- No.

¿Se realiza mantenimiento de inventario para recurso de información, recursos de software, recursos físicos y servicios?

- Sí.
- No.

¿El esquema de la clasificación del inventario permite el hecho de que la importancia de la información pueda cambiar (Posiblemente de acuerdo con una política predeterminada)?

- Sí.
- No.

¿Se asigna un código de registro (se etiqueta) a la información clasificada para llevar un control de ella?

- Sí.
- No.

¿Los informes impresos, *Screen Displays*, soportes magnéticos, mensajes electrónicos y transferencias de archivos tienen un código de registro y se clasifican apropiadamente?

- Sí.
- No.

¿Los procedimientos que se llevan a cabo en centros de procesamiento de información se encuentran documentados y clasificados según su importancia?

- Sí.
- No.

¿Los procesos de copiado, almacenamiento, transferencia electrónica, transmisión de voz y destrucción de información, tiene procedimientos del manejo de la información?

- Sí.
- No.

Práctica. Asignación de responsabilidades de los activos.

¿Se incluye en la política de seguridad el manejo de las responsabilidades generales y específicas en todos los aspectos de la seguridad de la información en la organización?

- Sí.
- No.

¿Todos los activos tienen un usuario responsable?

- Sí.
- No.

Proceso:

Administración de problemas e incidentes

Metas, criterios de evaluación y prácticas:

Meta: Documentar los incidentes de seguridad de la información.

Criterios de evaluación:

Práctica: Creación y diseño de una política de manejo de incidentes.

¿Hay una política definida para el manejo de los incidentes de la seguridad de la información?

- Sí.
- No.

¿La política contiene una explicación del proceso para divulgar los incidentes sospechosos de seguridad?

- Sí.
- No.

¿La política para el manejo de incidentes detalla los roles y responsabilidades en la identificación y manejo de dichos incidentes?

- Sí.
- No.

¿Se tiene establecido en la política para el manejo de incidentes la cancelación de los accesos a los sistemas de información cuando se terminan los contratos o son retirados los empleados de la organización?

- Sí.
- No.

¿Están todos los usuarios informados de su rol en el manejo en los incidentes de seguridad?

- Sí.
- No.

¿El procedimiento de manejo de incidentes incluye una clasificación de los tipos de incidentes de seguridad y sus respectivos planes de acción en caso de ocurrencia?

- Sí.
- No.

¿Hay un mecanismo para supervisar y para cuantificar los tipos, la cantidad, y los costes de incidentes de la seguridad de la información y de errores de sistema?

- Sí.
- No.

¿El procedimiento para la administración de incidentes detalla las acciones que deben ser realizadas al preparar el seguimiento a un incidente serio?

- Sí.
- No.

¿Existe un procedimiento para la entrega de los activos de la empresa por parte del empleado cuando es despedido o finaliza su contrato?

- Sí.
- No.

Práctica: Definición de medidas disciplinaria.

¿La política para el manejo de incidentes también destaca las acciones disciplinarias que serán tomadas contra el personal que se encontró responsable de causar deliberadamente un incidente?

- Sí.
- No.

¿Existe un procedimiento formal para tratar al personal que se ha encontrado violando las políticas y procedimientos de seguridad de la organización?

- Sí.
- No

¿Existe un procedimiento definido para el despido o traslado de un empleado, y este procedimiento está dentro de las políticas de la seguridad de la información?

- Si.
- No.

Proceso:

Definición del plan de continuidad de TI.

Metas, criterios de evaluación y prácticas:

Meta: Documentar y proteger adecuadamente el plan de continuidad del negocio.

Criterios de evaluación:

Práctica: Diseño del plan de continuidad.

¿Hay un proceso establecido en la organización para desarrollar y mantener la continuidad del negocio?

- Sí.
- No.

¿El proceso de planeación para el diseño del plan de continuidad incluye el análisis de riesgo de los procesos críticos del negocio?

- Sí.
- No.

¿Las responsabilidades y órdenes de emergencia están identificadas y acordadas?

- Sí.
- No.

¿El plan de continuidad se ha desarrollado para mantener o para restaurar las operaciones del negocio en los niveles de tiempo requerido, luego de interrupciones o fallas en los procesos críticos del negocio?

- Sí.
- No.

¿La implementación del plan de continuidad incluye la compra de seguros para los activos de la organización?

- Sí.
- No.

¿Se tiene documentado la estrategia y los planes de continuidad del negocio?

- Sí.
- No.

¿Se cuenta con procedimientos de emergencias y de reanudación de operaciones dentro del plan de continuidad del negocio?

- Sí.
- No.

¿Existen responsabilidades claras y definidas en el plan de continuidad del negocio en caso de emergencias y/o reanudación de operaciones?

- Sí.
- No.

¿Se cuenta con un cronograma de mantenimiento para el plan de continuidad del negocio?

- Sí.
- No.

¿El proceso incluye concientización y capacitación del personal?

- Sí.
- No.

7.4 NIVEL 3 (DEFINIDO)

Existe un sistema de gestión de seguridad de la información, documentado y estandarizado dentro de la organización. Todos los controles son debidamente documentados, aprobados, implementados, probados y actualizados.

Proceso:
Administración del Recurso Humano

Metas, criterios de evaluación y prácticas:

Meta: Lograr que la seguridad de la información sea tenida en cuenta en los procesos de la empresa.

Criterios de evaluación:

Práctica: Incorporación de la seguridad de la información en la organización.

¿Los administradores se aseguran que los empleados, contratistas y empleados Outsoursing apliquen la seguridad de acuerdo con las políticas de la organización?

- Sí.
- No.

¿Se realizan campañas de seguridad en la organización para incentivar el correcto uso de los equipos de cómputo y los sistemas de información?

- Sí.
- No.

Práctica: Proceso de selección, contratación y promoción.

¿Existen procesos para la selección de empleados?

- Sí.
- No.

¿Se realiza un proceso de selección para los contratistas y el personal temporal (directamente o a través de una cláusula en el contrato con las empresas proveedoras)?

- Sí.
- No.

¿Los empleados, contratistas, y los empleados Outsoursing firman los términos y las condiciones que contienen las responsabilidades de la seguridad de la información?

- Sí.
- No.

Al momento de cubrir una vacante con un empleado de la organización, ¿se tienen en cuenta las capacidades y el rendimiento de los postulantes?

- Sí.
- No.

¿Se brinda a los nuevos empleados la capacitación necesaria para desarrollar de manera apropiada sus funciones dentro de la organización?

- Sí.
- No.

Proceso:

Responsabilidad de la seguridad lógica y física

Metas, criterios de evaluación y prácticas:

Meta: Asignar responsabilidades de los activos físicos y lógicos existentes en todos los niveles de la organización buscando de esta manera preservar la seguridad de la información.

Criterios de evaluación:

Práctica: Asignación de responsabilidades.

¿La responsabilidad de la seguridad se mira como un asunto del negocio, y se acepta como tal, y esto tiene una contribución de todas las partes del equipo de la gerencia de la organización?

- Sí.
- No.

¿Las responsabilidades de administración, actualización, mantenimiento, asignación de accesos, de todos los activos físicos y lógicos está concentrada en cabeza de la Gerencia de TI?

- Sí.
- No.

Si las responsabilidades de los activos físicos y lógicos de la organización no se concentran en la Gerencia de TI, ¿estas responsabilidades recaen en niveles gerenciales dentro de la organización?

- Sí.
- No.

¿Existe documentación donde se evidencie la aceptación de las responsabilidades en el manejo de los activos físicos y lógicos dentro de la organización?

- Sí.
- No.

Proceso:
Implementación de controles e indicadores de medición.

Metas, criterios de evaluación y prácticas:

Meta: La organización establece controles para proteger tanto los activos físicos como los lógicos, dentro y fuera de la organización, e inicia una implementación de indicadores que permitan evaluar la efectividad de estos controles.

Criterios de evaluación:

Práctica: Implementación de controles de acceso.

¿Está considerado dentro de la política de control de accesos la segregación de roles, la validez del autor de la petición de acceso, la revisión periódica y la remoción de derechos de acceso?

- Sí.
- No.

¿La política de control de acceso está alineada con la política de la clasificación de los activos?

- Sí.
- No.

¿Está considerado dentro de la política de acceso la difusión de información?

- Sí.
- No.

¿Hay perfiles estándares de acceso de usuario (para cargos operativos que realicen las mismas funciones) para las categorías comunes de trabajo?

- Sí.
- No.

¿Hay un sistema de registro formal para el acceso a los servicios de procesamiento de información?

- Sí.
- No.

¿El procedimiento de registro de usuarios garantiza que estos solo accedan a las operaciones autorizadas, además realiza la correcta validación del usuario con su identificador único y su respectiva contraseña y guarda registro de este procedimiento?

- Sí.
- No.

¿Están las instalaciones para el procesamiento de la información protegidas contra el acceso no autorizado, daños e interferencias, localizándolas en áreas seguras?

- Sí.
- No.

¿Las rutinas del sistema se desarrollan para evitar la necesidad de conceder privilegios a los usuarios?

- Sí.
- No.

¿Los controles de acceso para el sistema operativo que controla las operaciones del negocio son apropiados en la organización?

- Sí.
- No.

¿Los usuarios tienen un identificador único para su uso personal?

- Sí.
- No.

¿Se desactivan las terminales (*time-out*) después de un período definido de inactividad para prevenir el acceso de personas no autorizadas?

- Sí.
- No.

¿Se restringen los programas utilitarios del sistema que pudieran ser capaces de eliminar los usos y controles del sistema y son rigurosamente controlados?

- Sí.
- No.

¿Las necesidades del negocio sobre el control de acceso se definen y se documentan?

- Sí.
- No.

¿Hay una declaración de política de acceso que define los privilegios de acceso de cada usuario o grupo de usuarios?

- Sí.
- No.

¿Se tiene una declaración escrita de los privilegios de acceso a la información (física y digital) la cual es leída y firmada por los usuarios para garantizar que entienden las condiciones?

- Sí.
- No.

¿Se recomienda a los usuarios de los equipos de cómputo que terminen la sesión y apaguen el sistema al finalizar la jornada y que aseguren su equipo con contraseña?

- Sí.
- No.

¿Se cuentan con indicadores que permitan identificar el número de reclamos debido a accesos desautorizados?

- Sí.
- No.

Práctica: Implementación de controles sobre red.

¿Las conexiones para los sistemas informáticos remotos se autentican?

- Sí.
- No.

¿Son autenticadas las conexiones a través de vías públicas (o redes fuera de la compañía) para usuarios remotos?

- Sí.
- No.

¿Los accesos remotos a los puertos de diagnóstico de seguridad se controlan con procedimientos que garanticen que solo son accesibles a los proveedores de soporte técnico autorizados y con los cuales existen convenios?

- Sí.
- No.

¿Las redes públicas son separadas en dominios lógicos diferentes a los de la red interna a través de un perímetro definido (por ejemplo un *firewall*) el cual restringe las capacidades de la conexión de los usuarios?

- Sí.
- No.

¿Existen controles para restringir a los usuarios la capacidad de la conexión a la red? (ej.: a través de un *gateways* que filtre el tráfico por medio de las tablas predefinidas)

- Sí.
- No.

¿Existen controles de enrutamiento que garanticen que las conexiones de los computadores y los flujos de información no violen las políticas de acceso a las aplicaciones del negocio?

- Sí.
- No.

¿El procedimiento de conexión limita los intentos de acceso a la red?

- Sí.
- No.

¿Las contraseñas que ingresan los usuarios son exhibidas en pantalla?

- Sí.
- No.

Cuando se autoriza el trabajo remoto, ¿se tiene en cuenta la seguridad física y el entorno de trabajo donde se realizará éste?

- Sí.
- No.

¿Se tiene identificada la información que se trasmite a través de la red para realizar los trabajos remotos y esta información está debidamente protegida?

- Sí.
- No.

¿Se cuenta con dispositivos (antivirus y f*irewall*) que garanticen la protección contra virus y accesos denegados al momento de realizar trabajos remotos?

- Sí.
- No.

¿Pueden los usuarios acceder solamente a los servicios de red que se les autorizaron utilizar?

- Sí.
- No.

¿Hay una política que se refiere al uso y servicios de las redes?

- Sí.
- No.

¿El trabajo remoto es autorizado por la gerencia y controlado específicamente para asegurar un nivel de protección conveniente?

- Sí.
- No.

¿Los tiempos de conexión para las funciones de riesgo elevadas son restringidos (por ejemplo a las horas de oficinas normales)?

- Sí.
- No.

¿Los administradores de la red han puesto controles en ejecución para garantizar la seguridad en las redes de datos y la protección de servicios conectados contra el acceso desautorizado?

- Sí.
- No.

¿Se cuentan con indicadores que permitan identificar el número de virus introducidos en la organización?

- Sí.
- No.

¿Se cuenta con indicadores que permitan identificar el número de ataques a la red de la organización?

- Sí.
- No.

Práctica: Implementación de controles en activos lógicos

¿Se valida que el ingreso de datos se encuentre dentro del rango de chequeo y no contenga caracteres inválidos?

- Sí.
- No.

¿Se realizan procedimientos de balanceo para los datos, tanto de entrada como de salida, para garantizar que no existan datos perdidos o incompletos?

- Sí.
- No.

¿Se verifica que el volumen de datos a cargar sea inferior a los límites de los equipos de almacenamiento?

- Sí.
- No.

¿Se realizan revisiones periódicas de los campos de entrada de datos y/o archivos?

- Sí.
- No

¿Se inspecciona que los *backup* concuerden con la información original?

- Sí.
- No

¿Se realizan procedimientos de validación de errores en los datos?

- Sí.
- No

¿El personal encargado de ingresar los datos conoce y acepta sus responsabilidades en este proceso?

- Sí.
- No

¿Se realizan chequeos en la integridad de los datos?

- Sí.
- No

¿Los datos se validan a través del ciclo del proceso?

- Sí.
- No.

¿Existe un procedimiento de validación para los datos generados por el sistema?

- Sí.
- No.

¿Son suficientes los controles de validación para asegurar la completitud, autenticidad y exactitud de los datos de entradas en las aplicaciones?

- Sí.
- No.

¿Las aplicaciones se ejecutan en el orden y tiempo correcto?

- Sí.
- No.

¿Existen *xfers*[16] para las transferencias electrónicas de información?

- Sí.
- No.

¿La autentificación de mensajes se utiliza para las aplicaciones que implican la transmisión de datos sensibles, para prevenir/detectar cambios no autorizados o alguna corrupción?

- Sí.
- No.

[16] *Ver glosario*

¿La actualización de software sobre los sistemas operativos es realizada solamente por los administradores?

- Sí.
- No.

¿En la actualización de software sobre el sistema operativo se utiliza solamente archivos ejecutables para este procedimiento?

- Sí.
- No.

¿Se registra quién realizó la actualización del software?

- Sí.
- No.

¿Cuándo se realiza una actualización de versiones de software, las anteriores son conservadas?

- Sí.
- No.

¿Cuándo se realiza una actualización de versiones se mantiene la configuración que se tenía?

- Sí.
- No.

¿El procedimiento de actualización de software está acorde con la estrategia de la organización?

- Sí.
- No.

¿Sólo el personal de informática tiene acceso al código fuente de las bibliotecas del programa?

- Sí.
- No.

¿Todas las actualizaciones al código fuente son autorizadas por el personal encargado?

- Sí.
- No.

¿Existe un procedimiento establecido para el control de cambios en el código fuente?

- Sí.
- No.

¿Se registra quién accedió al código fuente de las bibliotecas de los programas?

- Sí.
- No.

Si un sistema es sensible de funcionar en un ambiente compartido, ¿se identifica y se ajustan los otros sistemas con los cuales compartirá recursos?

- Sí.
- No.

¿Los intercambios de información y de software con otras organizaciones se controlan formalmente?

- Sí.
- No.

Práctica: Implementación de controles sobre las contraseñas.

¿La asignación de las contraseñas de los usuarios se controla?

- Sí.
- No.

¿Se requiere que los usuarios firmen un compromiso para cuidar su contraseña?

- Sí.
- No.

¿El usuario confirma el recibo de la nueva contraseña y el sistema obliga a su cambio la primera vez que ingresa a éste por una nueva contraseña que debe ser única?

- Sí.
- No.

¿Las contraseñas se transportan a través de medios seguros (correos certificados)?

- Sí.
- No.

¿Los sistemas muestran al usuario mensajes de advertencia donde se recuerda no crear contraseñas de fácil recordación?

- Sí.
- No.

Práctica: Implementación de claves criptográficas y llaves digitales.

¿El uso de los servicios de no-repudio (servicio que permite probar la participación de las partes en una comunicación) ha sido considerado donde pueda ser necesario resolver conflictos sobre la ocurrencia o la no-ocurrencia de una transmisión de información?

- Sí.
- No.

¿La política de la organización incluye el uso de controles criptográficos para la protección de la información?

- Sí.
- No.

¿La estimación del riesgo se utiliza para determinar qué control criptográfico es apropiado?

- Sí.
- No.

¿Se considera el tipo/calidad del algoritmo y la longitud de las claves en las herramientas de protección criptográfica?

- Sí.
- No.

¿Se consideran las restricciones/regulaciones locales y la exportación e importación de controles para la protección criptográfica?

- Sí.
- No.

¿Las claves criptográficas tienen fechas definidas para su activación y desactivación?

- Sí.
- No.

¿Todas las llaves criptográficas se protegen contra la modificación y la destrucción, y en el caso de las llaves privadas se protegen contra el acceso a éstas?

- Sí.
- No.

¿Se ha considerado el uso de certificados de claves públicas, avaladas por una autoridad certificada y reconocida para asegurar la protección de éstas?

- Sí.
- No.

Proceso:

Administración de Instalaciones.

Metas, criterios de evaluación y prácticas:

Meta: La organización establece controles tanto internos como externos para proteger las instalaciones.

Criterios de evaluación:

Práctica: Implementación de controles en instalaciones.

Para las áreas que contienen instalaciones para el procesamiento de información, ¿se tienen definidos perímetros de seguridad con pisos y techos protegidos por barreras, acondicionados con puertas de incendio, sistemas de detección de intrusos y ventanas de seguridad (si estas áreas se encuentran en primeros pisos)?

- Sí.
- No.

¿Las áreas claves son convenientemente localizadas y protegidas para reducir los riesgos de amenazas y de peligros ambientales, y para reducir las oportunidades para el acceso no autorizado?

- Sí.
- No.

Cuando es necesario el acceso de un visitante, ¿se registra el acceso de este a las áreas sensibles, se revoca el acceso al finalizar su visita y es constantemente supervisado?

- Sí.
- No.

¿Es apropiado el equipo contra incendios localizado en todas las áreas?

- Sí.
- No.

¿Se tiene prohibido comer, tomar o fumar en las áreas de procesamiento de información?

- Sí.
- No.

¿Están las instalaciones para el tratamiento de la información protegidas contra apagones (utilizando sistemas de alimentación interrumpidas o plantas eléctricas) u otras anomalías eléctricas (utilizando estabilizadores)?

- Sí.
- No.

¿Es adecuado el abastecimiento de agua y es estable para apoyar sistemas de aire acondicionado, manejo de la humedad y del fuego?

- Sí.
- No.

Práctica: Administración de instalaciones.

¿Existe una política formal en la organización donde se asegure el buen uso de instalaciones móviles (Ejemplo: *palmtops,* computadoras portátiles, teléfonos móviles, redes inalámbricas)?

- Sí.
- No.

¿El mantenimiento a los equipos de cómputo es realizado por personal autorizado, se ejecuta en intervalos de tiempos recomendados y se registran los daños encontrados?

- Sí.
- No.

Proceso:

Seguimiento de problemas y *logs* de Auditoría

Metas, criterios de evaluación y prácticas:

Meta: Se identifican e implementan los registros y herramientas que permitan realizar las labores propias de Auditoría.

Criterios de evaluación:

Práctica: Registros de elementos para auditoría

¿Los sistemas de información están supervisados y los eventos de seguridad de la información se registran?

- Sí
- No.

¿Toda la actividad de monitoreo y de auditoría cumplen con requisitos legales y mejores practicas establecidas, tales como IIA, ISO y/o COBIT?

- Sí.
- No.

¿Los registros de la auditoría se producen y se conservan por un período de tiempo convenido?

- Sí.
- No.

¿Los registros de monitoreo de actividades se protegen contra la modificación y el acceso no autorizados, incluyendo administradores de sistemas con privilegios de gran alcance?

- Sí.
- No.

¿Los registros son revisados sobre una base regular por un revisor independiente?

- Sí.
- No.

¿Los errores de sistema, las fallas de acceso al sistema y los "*logs*" son revisados regularmente, y se toman acciones correctivas?

- Sí.
- No.

¿Los relojes del sistema se sincronizan con una fuente exacta de tiempo para controlar los registros de auditoría?

- Sí.
- No.

7.5 NIVEL 4 (GESTIONADO CUANTITATIVAMENTE)

La organización realiza auditorías al sistema de gestión de seguridad de la información y recolecta métricas para establecer la efectividad de los controles.

Proceso:
Implementación y evaluación del plan de continuidad

Metas, criterios de evaluación y prácticas:

Meta: La organización trabaja continuamente en la conservación de la seguridad de la información a través de revisiones y modificaciones constantes a los planes de continuidad del negocio.

Criterios de evaluación:

Práctica: Revisión y actualización del plan de continuidad.

¿El plan de continuidad se revisa en periodos entre 6 y 9 meses?

- Sí.
- No.

¿El proceso de continuidad del negocio incluye la revisión y actualización del plan para asegurar la eficacia continua?

- Sí.
- No.

Proceso:

Monitoreo del Proceso.

Metas, criterios de evaluación y prácticas:

Meta: La organización evalúa el correcto funcionamiento de los procesos de TI.

Práctica: Implementación de indicadores para medir los procesos.

¿Se cuenta con reportes desarrollados a partir de los indicadores de medición donde se presenta el desempeño de los procesos de TI?

- Sí.
- No.

¿Se realizan encuestas para evaluar la satisfacción de los clientes acerca de los procesos de TI?

- Sí.
- No.

¿Se registra el tiempo entre la notificación de una deficiencia y el inicio de su acción correctiva?

- Sí.
- No.

¿Se tiene un indicador acerca de total de procesos monitoreados en la organización?

- Sí.
- No.

Proceso:

Administración de controles.

Metas, criterios de evaluación y prácticas:

Meta: La organización trabaja continuamente en la conservación de la seguridad de la información a través de revisiones continuas a los controles implementados.

Práctica: Administración de accesos.

¿Hay un proceso de autorización para conceder privilegios y se mantiene un *log* de todos los privilegios asignados?

- Sí.
- No.

¿Las autorizaciones de acceso a los sistemas se revisan en intervalos regulares?

- Sí.
- No.

¿Las capacidades de acceso de usuarios a los sistemas son revisadas en periodos entre los 6 y 8 meses?

- Sí.
- No.

¿Las autorizaciones para los privilegios de acceso son revisadas en periodos comprendidos entre 2 y 4 meses?

- Sí.
- No.

¿Los cambios de control de acceso para las cuentas privilegiadas se registran?

- Sí.
- No.

¿La asignación de privilegios se comprueba en intervalos de tiempo regulares?

- Sí.
- No.

¿Las guías de las buenas prácticas determinadas por la gerencia son comunicadas a los usuarios según sus responsabilidades en el aseguramiento, particularmente en la asignación y uso de contraseñas, la protección del equipo desatendido, y la importancia de una política de “escritorio limpio”?

- Sí.
- No.

¿Las cuentas de los usuarios que cambian de funciones o son retirados de la organización, son removidas inmediatamente?

- Sí.
- No.

Práctica: Administración de contraseñas.

¿Los sistemas validan que las contraseñas se cambien regularmente por otras cuya longitud no sea inferior a seis caracteres y no haya sido recientemente utilizada?

- Sí.
- No.

¿Al momento en que un usuario recibe su contraseña, el sistema obliga al inmediato cambio de esta luego de la primera conexión?

- Sí.
- No.

¿Las contraseñas son confidenciales e individuales (únicas para cada usuario)?

- Sí.
- No.

Cuando se escribe la contraseña en los sistemas, ¿esta no se exhibe en pantalla y tiene cifrado sostenido?

- Sí.
- No.

¿Se sugiere a los usuarios, para el mantenimiento de las contraseñas, al menos tres de los siguientes consejos: Nunca escriba su contraseña. (Memorícela), no cree una contraseña de fácil adivinación, nunca almacene la contraseña como una macro, nunca comparta la contraseña o no use palabras de diccionario?

- Sí.
- No.

Práctica: Control de los datos para pruebas.

¿Existen controles para el acceso a los sistemas de prueba de datos?

- Sí.
- No.

¿Se aplican los mismos controles de accesos tanto a los datos de prueba como a los reales?

- Sí.
- No.

¿Se tienen diferentes autorizaciones de acceso para los datos de prueba y para los datos reales?

- Sí.
- No.

¿Son borrados los datos de pruebas luego de realizadas éstas?

- Sí.
- No.

¿Se guardan registros de la utilización de datos reales para la realización de pruebas?

- Sí.
- No.

Práctica: Administración de herramientas para garantizar la confiabilidad en las trasmisiones de información.

¿Existe un sistema de administración de claves conveniente en la organización, basado sobre un sistema de estándares, procedimientos y de métodos seguros?

- Sí.
- No

¿Se toma el cuidado apropiado para proteger la integridad y la confidencialidad de las claves privadas cuando se emplean firmas digitales?

- Sí.
- No.

¿Se han dado todas las consideraciones correspondientes a los aspectos legislativos sobre el estado y uso de firmas digitales?

- Sí.
- No.

Proceso:

Monitoreo del control interno

Metas, criterios de evaluación y prácticas:

Meta: La organización desarrolla y fortalece programas de auditoría para mantener el control interno dentro de ella.

Práctica: Definición de la auditoría dentro de la organización.

¿Las auditorías de los sistemas operacionales se planean, se ajustan y se realizan de una manera controlada (que reduce al mínimo el riesgo de la interrupción del proceso del negocio)?

- Sí.
- No.

¿La política de auditoría de los sistemas de información está acorde con los requisitos de la gerencia?

- Sí.
- No.

¿La política de auditoría de los sistemas de información restringe el acceso al auditor a solo lectura para el software y los datos, y se monitorean y registran sus accesos?

- Sí.
- No.

¿La política de auditoría de los sistemas de información determina la disponibilidad de los recursos para realizar dicha actividad?

- Sí.
- No.

¿Los procedimientos de auditoría están debidamente documentados?

- Sí.
- No.

¿Dentro de la política de auditoría de los sistemas de información existen acuerdos para ejecuciones especiales?

- Sí.
- No.

¿Se incluyen los servicios de auditores independientes o externos dentro de la política de auditoría de los sistemas de información?

- Sí.
- No.

¿Los hallazgos encontrados en los procedimientos de revisión son reportados a un nivel adecuado de la organización; esto es, se informa a la persona encargada de la función que tuvo el inconveniente y a su jefe inmediato?

- Sí.
- No.

7.6 NIVEL 5 (EN OPTIMIZACIÓN).

Existe una mejora continua del sistema de gestión de seguridad de la información, basada en la realimentación cuantitativa y cualitativa de las auditorías al sistema de seguridad de la información.

Proceso:
Afinamiento y mantenimiento del plan de continuidad

Metas, criterios de evaluación y prácticas:

Meta: Mantener el plan de continuidad lo más actualizado posible frentes a los cambios significativos que se den en la organización y en su entorno.

Criterios de evaluación:

Práctica: Mejoramiento continuo.

¿Los cambios significativos internos (en los sistemas o aplicaciones, el personal, la ubicación física o en los procesos claves del negocio) conllevan una revisión del plan de continuidad del negocio?

- Sí.
- No.

¿Los cambios externos (contratos convenidos con otras organizaciones, legislativos o de proveedores) conllevan una revisión del plan de continuidad del negocio?

- Sí.
- No.

¿El plan de continuidad es revisado y actualizado en periodos comprendidos entre los 6 y 8 meses?

- Sí.
- No.

Si el plan de continuidad se ejecutó ante alguna eventualidad, ¿se realiza alguna retroalimentación para evaluar los puntos en que se pueda mejorar?

- Sí.
- No.

Proceso:

Evaluar lo adecuado del Control Interno.

Metas, criterios de evaluación y prácticas:

Meta: Asegurar el cumplimiento de los objetivos del control interno establecidos para los procesos.

Criterios de evaluación:

Práctica: Revisión del control interno.

¿La gerencia revisa los puntos vulnerables y problemas de seguridad reportados por el monitoreo continuo de los controles internos?

- Sí.
- No.

¿La gerencia tiene identificadas las fuentes que suministran la información necesaria para la toma de decisiones acerca de los eventos de control interno?

- Sí.
- No.

¿Se mide el tiempo de respuesta entre la deficiencia del control interno y su notificación a la alta gerencia?

- Sí.
- No.

¿Se tiene establecido reportes del cumplimiento del control interno?

- Sí.
- No.

¿Se realiza auditorías externas de forma periódica?

- Sí.
- No.

¿Son los informes de las auditorías externas revisados por la alta gerencia y se toman las medidas correspondientes sobre sus recomendaciones?

- Sí.
- No.

Proceso:

Reportes Gerenciales del monitoreo del proceso.

Metas, criterios de evaluación y prácticas:

Meta: Mantener informada a la alta gerencia acerca del cumplimiento de los objetivos pactados y se toman decisiones con base en estos.

Criterios de evaluación:

Práctica: Informar a la alta gerencia del cumplimiento de metas establecidas.

¿Existen reportes gerenciales que indiquen el avance de la organización con respecto al logro de los objetivos planeados, la obtención de productos, el cumplimiento de los objetivos planteados y la mitigación de riesgos?

- Sí.
- No.

¿Se guían los planes de acción de la alta gerencia con respecto a le seguridad de la información con base en los reportes existentes?

- Sí.
- No.

Proceso:

Reportes de violación y actividades de seguridad.

Metas, criterios de evaluación y prácticas:

Meta: Monitorear constantemente los eventos que ponen en riesgo la información.

Criterios de evaluación:

Práctica: Reportar actividades de seguridad.

¿Las violaciones y las actividades de seguridad son registradas, reportadas y escaladas apropiadamente por parte de los encargados de la administración de los servicios de información, en forma regular, para de esta manera identificar y resolver actividades no autorizadas?

- Sí.
- No.

¿Se analizan los reportes de violaciones para identificar puntos críticos que puedan ser resueltos por la gerencia de TI?

- Sí.
- No.

APÉNDICE A: TRABAJO DE CAMPO.

Este es trabajo de campo realizado en la empresa Reimpex S.A con el fin de probar el modelo desarrollado.

Se decidió realizar el trabajo de campo en dicha empresa debido a su crecimiento sostenido en el sector textil, destacándose principalmente en la elaboración de marquillas y estampados, la ejecución de un plan de mejoramiento de infraestructura de TI, y a que la empresa se encuentra en un proceso para obtener la certificación de ISO 9001.

A continuación se presenta la metodología de trabajo que se llevó a cabo y los resultados obtenidos en este.

METODOLOGÍA DEL TRABAJO DE CAMPO

Para comenzar con la validación del modelo de madurez propuesto, se accedió a esta empresa ya que tenía un perfil tipo PyME (Pequeña y mediana empresa) y se podrían hacer las correcciones necesarias dentro del modelo, y además esta empresa estaba en proceso de certificación de la norma de calidad ISO 9001 versión 2000, lo cual les ha ayudado a implementar ciertos controles en el área de informática que son válidos dentro de los criterios de evaluación del modelo de seguridad de la información.

Antes de realizar la evaluación de la seguridad de la información, se empezó a conocer lo que hace la empresa y el sector en donde se desenvuelve. Luego, se indagó acerca de cómo estaba conformada la empresa y más específicamente el área de informática. Nos dimos cuenta que esta área es muy pequeña pero muy importante para el funcionamiento de los procesos críticos de la empresa, como la facturación y las ordenes hechas por los clientes para producir los adhesivos y las marquillas. Posteriormente, preguntamos sobre toda la tecnología (software y hardware) que tiene la empresa y de qué forma se utiliza para el buen funcionamiento de esta, y durante la evaluación, nos iban contando las distintas anécdotas e inconvenientes que han tenido con los sistemas y cómo han afectado los procesos críticos.

ACTIVIDADES / DÍAS	1	2	3	4	5	6	7	8	9	10
Investigar empresas que se ajusten a la evaluación y que se tenga contactos										
Concretar la visita inicial para explicar el trabajo de campo										
Analizar la empresa y el área de informática										
Realizar la evaluacion de acuerdo con los criterios establecidos										
Revisar el modelo de seguridad de la información										
Establecer el nivel en que quedó la empresa, destacando fortalezas y áreas de oportunidad de mejora, suministrar conclusiones y recomendaciones.										

EMPRESA: REIMPEX S.A

SECTOR: Industria Textil.

REIMPEX es una empresa que lleva más de 40 años atendiendo a las grandes empresas textileras colombianas en sus necesidades de insumos en las áreas de hilatura y teneduría. Han ampliado su portafolio a diversos tipos de industria, como alimenticia, papelera, artes gráficas y confección.

El compromiso de REIMPEX con sus clientes ha sido brindarles seguridad y confiabilidad al proveerlos con insumos de excelente calidad a precios competitivos y entregar un valor agregado como es el servicio, el cual es quizás más importante que el producto en si.

Este valor agregado ha sido gracias al grupo humano de REIMPEX que se esmera en estudiar en forma permanente cómo mejorar y mantener el mejor nivel de servicio al cliente que cualquier empresa pueda brindar.

Por eso, actualmente están en el proceso de implementación del sistema de gestión de calidad ISO 9001 versión 2000.

MISIÓN

Entregar a nuestros clientes soluciones integrales, destacándonos por el alto nivel de servicio, precios competitivos y productos muy calificados.

VISIÓN.[17]

Alcanzar a diciembre del 2006 un crecimiento en las ventas de nuestro portafolio de productos y una mayor participación en el mercado nacional con énfasis en Medellín y Bogotá; en este mismo periodo lograr solidez financiera, el bienestar social y el crecimiento profesional de nuestros colaboradores, y una sincronización de los procesos por medio de la implementación del Sistema de Gestión de la Calidad

ESTADO ACTUAL DE LA EMPRESA EN TECNOLOGÍAS DE INFORMACIÓN

El área de informática de REIMPEX cuya sede principal se encuentra en la ciudad de Medellín, está a cargo de la Ingeniera Diana Patricia López quien cuenta con el soporte de los distintos proveedores de tecnología con los cuales la empresa tiene convenios. Esta área brinda soporte y servicio principalmente al Departamento Administrativo de la empresa (Contabilidad, facturación, elaboración de pedidos y compras) que cuenta con 20 usuarios, y al área operativa o de producción, donde se encargan de elaborar las marquillas, etiquetas y adhesivos. Adicionalmente, la empresa tiene una sede en Bogotá D.C, donde toda la transmisión de información se realiza por medio de correo electrónico (*email*).

El área de informática cuenta con los siguientes elementos:

- Un servidor Windows Small Bussines 2000 que cuenta con base de datos SQL Server para las aplicaciones de ofimática y con un *firewall* corporativo ISA Server para proteger la red con puertos cerrados de entrada y accesos denegados para Internet.

- 15 equipos con Microsoft Windows XP Proffesional y 5 equipos con Windows 98. Estos 5 equipos están en proceso de migración a Windows Vista.

[17] Actualmente no se cuenta con la visión actualizada.

- Software de ofimática Atlas cliente/servidor el cual es el más utilizado por la organización. Este aplicativo no fue hecho a la medida, ya que es un producto comercial, sin embargo se han realizado trabajos *in house* para ajustarlo.

- Antivirus McAfee.

- Software comercial para la transmisión y recepción de documentos EDI. Este software se le añadió un componente adicional desarrollado por el área de informática para que pudiera enviar y recibir documentos EDI a otra organización.

- En el área de producción se cuenta con impresoras QLS (*Quick Label System)* trabajan sobre un lenguaje de programación llamado *CQL* que maneja archivos planos y de tipo Excel como formatos de entrada, y otras impresoras de marca Zebra con las cuales se hacen las etiquetas, los adhesivos y maneja el lenguaje de programación para microprocesadores PLC (*Programmable Logic Controller*). Todos los archivos de entrada para ambos tipos de máquinas se almacenan en formato de Excel.

- En la infraestructura de la red se cuenta con un *rack* con todos los *switches*. En la red se tiene un espacio dentro del servidor destinado a los usuarios con su respectiva carpeta para uso diario.

- Los *backups* se realizan en CD´s y son de aproximadamente 4 MB (*Megabytes*) diarios. El *backup* se realiza semanal, además de tener la información diaria en la red. Recientemente se compró un disco externo para este proceso.

- Se cuenta con servicio externos (asesores que dan soporte a la aplicación administrativa), *testing* o escaneo de puertos. El proveedor encargado del mantenimiento del servidor no es siempre el mismo ya que no han estado satisfechos con algunos. También cuentan con proveedores de desarrollo de software para los requerimientos que se van presentando.

RESULTADOS DEL TRABAJO DE CAMPO.

Finalizada la evaluación de la metodología, se determinó que la organización REIMPEX S.A:

- Cumple a conformidad el nivel 0 (Básico), evidenciando que en la organización se viene inculcando una cultura de compromiso frente al manejo de la información; además, se tiene amplio apoyo de la alta gerencia, quienes comprenden la importancia de la seguridad de la información y participan en la implementación de medidas que colaboren con ella. Por último, cabe destacar que debido al proceso de certificación de la norma ISO 9001 que se está llevando a cabo en la organización, ya se tienen establecidos y documentados los procesos de negocio.

- Logra todos los objetivos del nivel 1 (Inicial), ya que se realiza una evaluación inicial de los activos que se tienen en la organización, además se tiene una identificación general de los riesgos que puede atentar contra los activos y se da un entrenamiento básico sobre la seguridad de la información.

- No alcanza a cumplir con todos los requisitos necesarios para el nivel 2 (Gestionado). Se recomienda:

    - Refinar el diseño de la política de seguridad en aspectos como la cuantificación de los riesgos identificados y el lineamiento de esta frente a aspectos legislativos y necesidades del negocio, a su vez se requiere que cuando la política sea revisada se guarde registro de los temas tratados para que sirvan como insumos para las próximas reuniones.

    - La creación de foros de seguridad y grupos Inter-funcionales que permitan a la organización mantenerse actualizada frente a los temas de seguridad y así mismo diseñar y desarrollar actividades.

    - Asignar un código visible a los activos de la organización ya sean físicos (PC`s, impresoras, equipos de red, etc.) o lógicos (*Screen Display*, mensajes electrónicos, etc.) para facilitar su ubicación y control, además

se recomienda establecer procedimientos para el almacenamiento, transferencia y destrucción de la información.

- Se deben definir roles y responsabilidades en caso de la ocurrencia de un incidente, además se debe contar con un mecanismo que permita guiar los pasos a seguir en caso de un incidente y cuantificar los costos asociados a este. Se deben establecer procedimientos para la entrega de los activos por parte de empleados que se encuentren implicados en un incidente de seguridad y se ha decidido retirarlos de la organización.

- Definir medidas disciplinarias y procedimientos formales que permitan tomar acciones frente a las personas involucradas en incidentes de la seguridad, dependiendo del grado y costo de estos incidentes.

- No se tienen implementados todos los procesos del nivel 3 (Definido), para esto se requiere:

  - Alinear la política de accesos con las necesidades de la empresa, implementar controles físicos y lógicos para el acceso a las instalaciones de procesamiento (servidor central y estaciones de trabajo), establecer acuerdos por escrito sobre los accesos permitidos a cada uno de los usuarios y diseñar indicadores que permitan conocer el comportamiento de los eventos de accesos no autorizados.

  - Se debe implementar acuerdos para el manejo, transporte y uso de las contraseñas.

  - Considerar en la política de la organización el uso de controles criptográficos.

  - Mejorar significativamente los controles y normas implementadas en las instalaciones de procesamiento de información, ubicando estas en sitios más seguros que garanticen su buen funcionamiento.

- Las actividades de monitoreo y auditoría deben estar alineadas con buenas prácticas tales como ISO y CoBit, recomendadas por organizaciones especializadas en temas de auditoría. Además se requiere de mayor cuidado en la revisión y conservación de los registros de auditoría.

- No cumple con los procesos del nivel 4 (Gestionado Cuantitativamente), por lo tanto se recomienda:

  - Revisar de manera periódica el plan de continuidad del negocio para garantizar la mejora continua de éste.

  - Implementar indicadores que permitan conocer el estado y funcionamiento de los procesos de TI.

  - Establecer un seguimiento más estricto de los controles de acceso implementados y a los privilegios concedidos.

  - Instaurar un ambiente de pruebas donde se establezca el correcto uso de la información y permita evaluar el software antes de implementarlo en la organización.

  - Garantizar el resguardo y buen uso de las claves digitales.

  - Se deben definir perfiles de auditor sobre los sistemas existentes, de tal manera que se restrinja el acceso a los datos para solo lectura y se protejan de su modificación. Además, es necesario incluir las actividades de auditorías externas en TI en la política de seguridad.

- No se tienen establecidos todos los procesos correspondientes al nivel 5 (En Optimización), por lo tanto se recomienda:

- Buscar el mejoramiento permanente del plan de continuidad teniendo en cuenta los cambios internos y del entorno (legislativos, proveedores, competencia).

- Que las decisiones tomadas por la alta gerencia sobre la seguridad de la información estén soportadas por los reportes referentes a los procesos de TI.

- Implementar mecanismo de administración de incidentes que permita escalarlos de manera apropiada y a su vez se evalúen de tal forma que puedan ser corregidas en el futuro.

APÉNDICE B: EVALUACIÓN DE LA METODOLOGÍA EN LA EMPRESA REIMPEX.S.A

NIVEL 0

Estos requisitos son indispensables para realizar la evaluación dentro de la organización.	
REQUISITOS	**CUMPLIMIENTO**
La alta gerencia está motivada para la implementación del modelo, esto es, que está dispuesta a apoyar con recursos necesarios tanto financieros como humanos.	SI
Los empleados se encuentran motivados y dispuestos a realizar dicha implementación, conocen el alcance y existen canales de comunicación establecidos dentro de la organización para difundir la información.	SI
Se tienen establecidos y documentados los procesos de negocio de la organización, sus responsables y una línea de autoridad definida.	SI
CUMPLIMIENTO DEL NIIVEL:	**CUMPLE EL NIVEL**

NIVEL 1

En este nivel la organización no ha realizado ninguna evaluación de riesgo que permita ver las falencias que se tienen en relación con la seguridad de la información, por lo tanto, los controles existentes fueron desarrollados de manera informal y la						
PROCESO	**META**	**PRÁCTICA**	**CRITERIO**	**APLICA**	**RESPUESTA**	**OBSRVACIÓN**
Reconocimiento de los sistemas	Documentar la clasificación de los activos de la organización (hardware, software, documentación física y electrónica, etc.) para darles la protección adecuada a cada uno de ellos.	Clasificación de activos físicos y lógicos.	¿Tienen los activos de la información alguna clasificación de Seguridad?	SI	SI	
			¿Existe algún esquema de clasificación de los activos lógicos y físicos de la organización y está debidamente documentado dicho esquema?	SI	SI	
			¿Esta clasificación de los activos se basa en la funcionalidad, costos, soporte a los procesos críticos del negocio, fortaleza y debilidades de estos?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			
Identificación del riego	Determinar el impacto que generan los eventos que atentan contra la información, los activos y la continuidad del negocio.	Identificación inicial del riesgo.	¿El proceso que evalúa y determina los riesgos a que está expuesta la organización comienza identificando los acontecimientos que pueden causar interrupciones a los procesos del negocio e incluyen el costo del impacto de estas interrupciones?	SI	SI	
			¿El análisis de riesgo a los que esta expuesta la organización tiene en cuenta los puntos de vista de la gerencia, la planeación estratégica, los resultados de las auditorias y los incidentes ocurridos?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			
Entrenamiento del personal	Diseñar programas de capacitación para los empleados, con los cuales se pueda dar a conocer los aspectos más importantes relativos a la seguridad.	Capacitación en seguridad y entrenamiento técnico.	¿Todos los usuarios han recibido una adecuada capacitación de seguridad y entrenamiento técnico?	SI	SI	
			¿La capacitación y el entrenamiento incluyen políticas y procedimientos de la organización, así como el uso correcto de las instalaciones de procesamiento de información antes de que se conceda el acceso a dichas instalaciones?	SI	SI	
			¿Estas actividades de entrenamiento se ejecutan de forma periódica para garantizar el aprendizaje continuo?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			
CUMPLIMIENTO DEL NIIVEL:	**CUMPLE EL NIVEL**					

NIVEL 2

Existen procesos básicos de gestión de la seguridad de la información. Los controles existentes hacen que se puedan detectar posibles incidentes de seguridad.						
PROCESO	**META**	**PRÁCTICA**	**CRITERIO**	**APLICA**	**RESPUESTA**	**OBSERVACIÓN**
Implementar y mantener las políticas de seguridad y garantizar la aprobación y apoyo por parte de la Gerencia.	Revisar y aprobar las Políticas de Seguridad de la información. Esta revisión debe ser hecha por los directivos de la organización.	Diseño de política de seguridad.	¿La política contiene una declaración de la intención de la gerencia que apoya las metas y los principios de la seguridad de la información?	SI	SI	
			¿La política contiene una definición de la seguridad de la información - sus objetivos y alcance totales - y de su importancia como mecanismo que permite administrar la información dentro de la organización?	SI	SI	
			¿La política contiene detalles de un marco de la seguridad (factores a evaluar), y un gravamen y programa de la gerencia de riesgo?	SI	NO	
			¿La política contiene una explicación de las reglas específicas de seguridad organizacional, los principios, los estándares y los requisitos de conformidad, de acuerdo con aspectos legislativos, políticas de la continuidad del negocio y consecuencias por violaciones?	SI	NO	
		CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
		Revisión de la política de seguridad.	¿Hay un proceso de revisión definido, que incluye responsabilidades y fechas de revisión para mantener el documento de la política?	SI	SI	
			¿La revisión de la política de seguridad incluye la evaluación de la eficacia de las políticas, el costo beneficio de los controles iniciales que se tienen y los cambios tecnológicos dados en la organización?	SI	SI	
			¿Quedan registrados los temas que se trataron el la revisión de la política de la seguridad en actas con las firmas de aprobación de la alta Gerencia para ser evaluadas en las próximas revisiones?	SI	NO	
		CUMPLIMIENTO DE PRACTICA:	CUMPLE			
		Asignar responsable de administrar la política.	¿La política tiene un dueño claro, el cual ha aceptado su responsabilidad en la administración de ésta, y esta aprobación queda registrada en un acta?	SI	SI	
			¿Se realizan actividades para aclarar dudas acerca de la política de seguridad comunicada a los empleados, para garantizar su comprensión?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Comunicación de las Intenciones y Aspiraciones de la Gerencia	Elaborar un plan para divulgar las Políticas de Seguridad de la información de la organización.	Distribución de la política de seguridad al personal correspondiente.	¿Existe un documento escrito de políticas de la seguridad conocido y disponible para TODO el personal en la organización responsable de la seguridad de la información?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			
Creación del grupo interdisciplinario de seguridad y relaciones con usuarios de TI	Establecer que las reuniones del grupo interdisciplinario sean lo más formal posible, es decir, se planeen y se dejen actas sobre los temas trabajados durante la reunión y sobre las acciones o compromisos pendientes, para el manejo de la información al interior de la organización.	Creación y definición de actividades del grupo interdisciplinario.	¿Existe dentro de la organización un foro de alto nivel (expertos en seguridad de la información internos y/o externos y representantes de la alta gerencia) para el manejo de la seguridad de la información para dar orientación y soporte a la administración?	SI	NO	
			¿Entre los temas tratados por el foro de seguridad de la información se tienen la revisión de las políticas de la compañía, el monitoreo de las amenazas de los activos, la revisión de los incidentes ocurridos y las sanciones de estos, y las actividades de seguridad que se desarrollaran, entre otros?	NO	SI	
		CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
		Creación del comité Inter-funcional y definición de sus actividades	¿Existe un comité Inter-funcional para coordinar medidas de seguridad de la información?	SI	NO	
			¿Entre los temas que son tratos por el comité Inter-funcional está el de determinar los roles y responsabilidades dentro de la organización, las iniciativas que se llevarán a cabo dentro de la organización sobre temas de seguridad, la coordinación e implementación de las nuevas medidas de seguridad y la revisión de los incidentes?	NO	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Evaluación y mantenimiento de los sistemas y datos existentes	Tener un inventario de los activos físicos y lógicos de la organización lo más completo posible.	Mantenimiento del inventario de los activos físicos y lógicos.	¿Existe mantenimiento al inventario de los activos de la organización?	SI	SI	
			¿Se realiza mantenimiento de inventario para recurso de información, recursos de software, recursos físicos y servicios?	SI	SI	
			¿El esquema de la clasificación del inventario permite el hecho de que la importancia de la información pueda cambiar (Posiblemente de acuerdo con una política predeterminada)?	SI	SI	
			¿Se asigna un código de registro (se etiqueta) a la información clasificada para llevar un control de esta?	SI	NO	
			¿Los informes impresos, Screen Displays, soportes magnéticos, mensajes electrónicos y transferencias de archivos tienen un código de registro y se clasifican apropiadamente?	SI	NO	
			¿Los procedimientos que se llevan a cabo en centros de procesamiento de información se encuentran documentados y clasificados según su importancia?	SI	SI	
			¿Los procesos de copiado, almacenamiento, transferencia electrónica, transmisión de voz y destrucción de información, tiene procedimientos del manejo de la información?	SI	NO	
		CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
		Asignación de responsabilidades de los activos.	¿Se incluye en la política de seguridad el manejo de las responsabilidades generales y específicas en todos los aspectos de la seguridad de la información en la organización?	SI	SI	
			¿Todos los activos tienen un usuario responsable?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Administración de Problemas e Incidentes	Documentar los incidentes de seguridad de la información.	Creación y diseño de una política de manejo de incidentes.	¿Hay una política definida para el manejo de los incidentes de la seguridad de la información?	SI	SI	
			¿La política contiene una explicación del proceso para divulgar los incidentes sospechosos de seguridad?	SI	SI	
			¿La política para el manejo de incidentes detalla los roles y responsabilidades en la identificación y manejo de dichos incidentes?	SI	NO	
			¿Se tiene establecido en la política para el manejo de incidentes la cancelación de los accesos a los sistemas de información cuando se terminan los contratos o son retirados los empleados de la organización?	SI	SI	
			¿Están todos los usuarios informados de su rol en el manejo en los incidentes de seguridad?	SI	SI	
			¿El procedimiento de manejo de incidentes incluye una clasificación de los tipos de incidentes de seguridad y sus respectivos planes de acción en caso de ocurrencia?	SI	SI	
			¿Hay un mecanismo para supervisar y para cuantificar los tipos, la cantidad, y los costes de incidentes de la seguridad de la información y de errores de sistema?	SI	NO	
			¿El procedimiento para la administración de incidentes detalla las acciones que deben ser realizadas al preparar el seguimiento a un incidente serio?	SI	NO	
			¿Existe un procedimiento para la entrega de los activos de la empresa por parte del empleado cuando es despedido o finaliza su contrato?	SI	NO	
		CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
		Definición de medidas disciplinaria.	¿La política para el manejo de incidentes también destaca las acciones disciplinarias que serán tomadas contra el personal que se encontró responsable de causar deliberadamente un incidente?	SI	NO	
			¿Existe un procedimiento formal para tratar al personal que se ha encontrado violando las políticas y procedimientos de seguridad de la organización?	SI	NO	
			¿Existe un procedimiento definido para el despido o traslado de un empleado, y este procedimiento está dentro de las políticas de la seguridad de la información?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Definición del plan de continuidad de TI.	Documentar y proteger adecuadamente el plan de continuidad del negocio.	Diseño del plan de continuidad.	¿Hay un proceso establecido en la organización para desarrollar y mantener la continuidad del negocio?	SI	SI	
			¿El proceso de planeación para el diseño del plan de continuidad incluye el análisis de riesgo de los procesos críticos del negocio?	SI	SI	
			¿Las responsabilidades y órdenes de emergencia están identificadas y acordadas?	SI	SI	
			¿El plan de continuidad se ha desarrollado para mantener o para restaurar las operaciones del negocio en los niveles de tiempo requerido, luego de interrupciones o fallas en los procesos críticos del negocio?	SI	SI	
			¿El diseño del plan de continuidad incluye la compra de seguros para los activos de la organización?	SI	SI	
			¿Se tiene documentado la estrategia y los planes de continuidad del negocio?	SI	SI	
			¿Se cuentan con procedimientos de emergencias y de reanudación de operaciones dentro del plan de continuidad del negocio?	SI	NO	
			¿Existen responsabilidades claras y definidas en el plan de continuidad del negocio en caso de emergencias y/o reanudación de operaciones?	SI	NO	
			¿Se cuenta con un cronograma de mantenimiento para el plan de continuidad del negocio?	SI	SI	
			¿El proceso incluye concientización y capacitación del personal?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			
CUMPLIMIENTO DEL NIIVEL:	**NO CUMPLE EL NIVEL**					

NIVEL 3

Existe un sistema de gestión de seguridad de la información, documentado y estandarizado dentro de la organización. Todos los controles son debidamente documentados, aprobados, implementados, probados y actualizados.						
PROCESO	**META**	**PRÁCTICA**	**CRITERIO**	**APLICA**	**RESPUESTA**	**OBSERVACIÓN**
Administración del Recurso Humano	Lograr que la seguridad de la información sea tenida en cuenta en los procesos de la empresa.	Incorporación de la seguridad de la información en la organización.	¿Los administradores se aseguran que los empleados, contratistas y empleados Outsoursing apliquen la seguridad de acuerdo con las políticas de la organización?	SI	SI	
			¿Se realizan campañas de seguridad en la organización para incentivar el correcto uso de los equipos de cómputo y los sistemas de información?	SI	NO	
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
		Proceso de selección, contratación y promoción.	¿Existen procesos para la selección de empleados?	SI	SI	
			¿Se realiza un proceso de selección para los contratistas y el personal temporal (directamente o a través de una cláusula en el contrato con las empresas proveedoras)?	SI	SI	
			¿Los empleados, contratistas, y los empleados Outsoursing firman los términos y las condiciones que contienen las responsabilidades de la seguridad de la información?	SI	SI	
			Al momento de cubrir una vacante con un empleado de la organización, ¿se tienen en cuenta las capacidades y el rendimiento de los postulantes?	SI	SI	
			¿Se brinda a los nuevos empleados la capacitación necesaria para desarrollar de manera apropiada sus funciones dentro de la organización?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	CUMPLE			
Responsabilidad de la Seguridad Lógica y física	Asignar responsabilidades de los activos físicos y lógicos existentes en todos los niveles de la organización buscando de esta manera preservar la seguridad de la información.	Asignación de responsabilidades.	¿La responsabilidad de la seguridad se mira como un asunto del negocio, y se acepta como tal, y esto tiene una contribución de todas las partes del equipo de la gerencia de la organización?	SI	SI	
			¿Las responsabilidades de administración, actualización, mantenimiento, asignación de accesos, de todos los activos físicos y lógicos esta concentrada en cabeza de la Gerencia de TI?	SI	SI	
			Si las responsabilidades de los activos físicos y lógicos de la organización no se concentran en la Gerencia de TI, ¿estas responsabilidades recaen en niveles gerenciales dentro de la organización?	SI	SI	
			¿Existe documentación donde se evidencie la aceptación de las responsabilidades en el manejo de los activos físicos y lógicos dentro de la organización?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Implementación de controles e indicadores de medición.	La organización establece controles para proteger tanto los activos físicos como los lógicos, dentro y fuera de la organización, e inicia una implementación de indicadores que permitan evaluar la efectividad de estos controles.	Implementación de controles de acceso	¿Esta considerado dentro de la política de control de accesos la segregación de roles, la validez del autor de la petición de acceso, la revisión periódica y la remoción de derechos de acceso?	SI	SI	
			¿La política de control de acceso esta alineada con la política de la clasificación de los activos?	SI	NO	
			¿Esta considerado dentro de la política de acceso la difusión de información?	SI	SI	
			¿Hay perfiles estándares de acceso de usuario (para cargos operativos que realicen las mismas funciones) para las categorías comunes de trabajo?	SI	SI	
			¿Hay un sistema de registro formal para el acceso a los servicios de procesamiento de información?	SI	NO	
			¿El procedimiento de registro de usuarios garantiza que estos solo accedan a las operaciones autorizadas, además realiza la correcta validación del usuario con su identificador único y su respectiva contraseña, y guarda registro de este procedimiento?	SI	SI	
			¿Están las instalaciones para el procesamiento de la información protegidas contra el acceso no autorizado, daños e interferencias, localizándolas en áreas seguras?	SI	NO	
			¿Las rutinas del sistema se desarrollan para evitar la necesidad de conceder privilegios a los usuarios?	SI	SI	
			¿Los controles de acceso para el sistema operativo que controla las operaciones del negocio son apropiados en la organización?	SI	SI	
			¿Los usuarios tienen un identificador único para su uso personal?	SI	SI	
			¿Se inactivan las terminales (*time-out*) después de un período definido de inactividad para prevenir el acceso de personas no autorizadas?	SI	NO	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Se restringen los programas utilitarios del sistema que pudieran ser capaces de eliminar los usos y controles del sistema y son rigurosamente controlados?	SI	NO	
			¿Las necesidades del negocio sobre el control de acceso se definen y se documentan?	SI	SI	
			¿Hay una declaración de política del acceso que define los privilegios de acceso de cada usuario o grupo de usuarios?	SI	SI	
			¿Se tiene una declaración escrita de los privilegios de acceso a la información (física y digital) la cual es leída y firmada por los usuarios para garantizar que entienden las condiciones?	SI	NO	
			¿Se recomienda a los usuarios de los equipos de cómputo que terminen la sesión y apaguen el sistema al finalizar la jornada y que aseguren su equipo con contraseña?	SI	SI	
			¿Se cuentan con indicadores que permitan identificar el número de reclamos debido a accesos desautorizados?	SI	NO	
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
		Implementación de controles sobre red.	¿Las conexiones para los sistemas informáticos remotos se autentican?	SI	SI	
			¿Son autenticadas las conexiones a través de vías públicas (o redes fuera de la compañía) para usuarios remotos?	SI	NO	
			¿Los accesos remotos a los puertos de diagnóstico de seguridad se controlan con procedimientos que garanticen que solo son accesibles a los proveedores de soporte técnico autorizados y con los cuales existen convenios?	SI	SI	
			¿Las redes públicas son separadas en dominios lógicos diferentes a los de la red interna a través de un perímetro definido (por ejemplo un *firewall*) el cual restringe las capacidades de la conexión de los usuarios?	SI	SI	
			¿Existen controles para restringir a los usuarios la capacidad de la conexión a la red? (ej.: a través de un *gateways* que filtre el tráfico por medio de las tablas predefinidas)	SI	SI	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Existen controles de enrutamiento que garanticen que las conexiones de los computadores y los flujos de información no violen las políticas de acceso a las aplicaciones del negocio?	SI	SI	
			¿El procedimiento de conexión limita los intentos de acceso a la red?	SI	SI	
			¿Las contraseñas que ingresan los usuarios son exhibidas en pantalla?	SI	SI	
			Cuando se autoriza el trabajo remoto,¿se tiene en cuenta la seguridad física y el entorno de trabajo donde se realizara este?	SI	SI	
			¿Se tiene identificada la información que se trasmite a través de la red para realizar los trabajos remotos y esta información esta debidamente protegida?	SI	SI	
			¿Se cuenta con dispositivos (antivirus y f*irewall*) que garanticen la protección contra virus y accesos denegados al momento de realizar trabajos remotos?		SI	
			¿Pueden los usuarios acceder solamente a los servicios de red que se les autorizaron utilizar?	SI	SI	
			¿Hay una política que se refiere al uso y servicios de las redes?	SI	NO	
			¿El trabajo remoto es autorizado por la gerencia y controlado específicamente para asegurar un nivel de protección conveniente?	SI	SI	
			¿Los tiempos de conexión para las funciones de riesgo elevadas son restringidos (por ejemplo a las horas de oficinas normales)?	SI	SI	
			¿Los administradores de la red han puesto controles en ejecución para asegurar la seguridad en las redes de datos y la protección de servicios conectados contra el acceso desautorizado?	SI	SI	
			¿Se cuentan con indicadores que permitan identificar el número de virus introducidos en la organización?	SI	NO	
			¿Se cuentan con indicadores que permitan identificar el número de ataques a la red de la organización?	SI	NO	
		CUMPLIMIENTO DE PRÁCTICA:	CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
		Implementación de controles en activos lógicos	¿Se valida que el ingreso de datos se encuentre dentro del rango de chequeo y no contenga caracteres inválidos?	SI	SI	
			¿Se realizan procedimientos de balanceo para los datos tanto de entrada como de salida para garantizar que no existan datos perdidos o incompletos?	SI	SI	
			¿Se verifica que el volumen de datos a cargar sea inferior a los límites de los equipos de almacenamiento?	SI	SI	
			¿Se realizan revisiones periódicas de los campos de entrada de datos y/o archivos?	SI	SI	
			¿Se inspeccionan que los backup concuerden con la información original?	SI	NO	
			¿Se realizan procedimientos de validación de errores en los datos?	SI	NO	
			¿El personal encargado de ingresar los datos conoce y acepta sus responsabilidades en este proceso?	SI	SI	
			¿Se realizan chequeos en la integridad de los datos?	SI	SI	
			¿Los datos se validan a través del ciclo del proceso?	SI	SI	
			¿Existe un procedimiento de validación para los datos generados por el sistema?	SI	SI	Por ejemplo saldo del inventario
			¿Las aplicaciones se ejecutan en el orden y tiempo correcto?	SI	SI	Más por política de la empresa
			¿Existen *xfers* para las transferencias electrónicas de información?	SI	SI	
			¿La autentificación de mensajes se utiliza para las aplicaciones que implican la transmisión de datos sensibles, para prevenir/detectar cambios no autorizados o alguna corrupción?	SI	SI	Aplicación contable y con el banco
			¿La actualización de software sobre los sistemas operativos es realizada solamente por los administradores?	SI	SI	
			¿En la actualización de software sobre el sistema operativo se utiliza solamente archivos ejecutables para este procedimiento?	SI	SI	
			¿Se registra quien realizó la actualización del software?	SI	SI	
			¿Cuándo se realiza una actualización de versiones de software, las anteriores son conservadas?	SI	SI	
			¿Cuándo se realiza una actualización de versiones se mantiene la configuración que se tenía?	SI	SI	
			¿El procedimiento de actualización de software esta acorde con la estrategia de la organización?	SI	SI	
			¿Solo el personal de informática tiene acceso al código fuente de las bibliotecas del programa?	SI	SI	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Todas las actualizaciones al código fuente son autorizadas por el personal encargado?	SI	SI	
			¿Existe un procedimiento establecido para el control de cambios en el código fuente?	SI	SI	
			¿Se registra quien accedió al código fuente de las bibliotecas de los programas?	SI	NO	Se escribe la fecha de modificación dentro del programa fuente
			¿Si un sistema es sensible de funcionar en un ambiente compartido, se identifica y se ajustan los otros sistemas con los cuales compartirá recursos?	SI	SI	
			¿Los intercambios de información y de software con otras organizaciones se controlan formalmente?	SI	SI	
		CUMPLIMIENTO DE PRÁCTICA:	CUMPLE			
		Implementación de controles sobre las contraseñas.	¿La asignación de las contraseñas de los usuarios se controla?	SI	SI	
			¿Se requiere que los usuarios firmen un compromiso para cuidar su contraseña?	SI	NO	
			¿El usuario confirma el recibo de la nueva contraseña y el sistema obliga a su cambio la primera vez que ingresa a este por una nueva contraseña que debe ser única?	SI	NO	
			¿Las contraseñas se transportan a través de medios seguros (correos certificados)?	SI	NO	
			¿Los sistemas muestran al usuario mensajes de advertencia donde se recuerda no crear contraseñas de fácil recordación?	SI	NO	
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
		Implementación de claves criptográficas y llaves digitales.	¿El uso de los servicios de no-repudio (servicio que permite probar la participación de las partes en una comunicación) ha sido considerado donde pueda ser necesario resolver conflictos sobre la ocurrencia o la no-ocurrencia de una transmisión de información?	SI	SI	Se tiene establecido con la DIAN y con los bancos.
			¿La política de la organización incluye el uso de controles criptográficos para la protección de la información?	SI	NO	
			¿La estimación del riesgo se utiliza para determinar qué control criptográfico es apropiado?	NO		
			¿Se considera el tipo/calidad del algoritmo y la longitud de las claves en las herramientas de protección criptográfica?	NO		
			¿Se considera las restricciones/regulaciones locales y la exportación e importación de controles para la protección criptográfica?	NO		
			¿Las claves criptográficas tienen fechas definidas para su activación y desactivación?	NO		

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Todas las llaves criptográficas se protegen contra la modificación y la destrucción, y en el caso de las llaves privadas, se protegen contra el acceso a éstas?	SI	SI	Las llaves se protegen en el servidor
			¿Se ha considerado el uso de certificados de claves públicas, avaladas por una autoridad certificada y reconocida para asegurar la protección de éstas?	NO	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
Administración de Instalaciones.	La organización establece controles tanto internos como externos para proteger las instalaciones.	Implementación de controles en instalaciones.	¿Para las áreas que contienen instalaciones para el procesamiento de información se tienen definidos perímetros de seguridad con pisos y techos protegidos por barreras, alarmado con puertas de incendio, sistemas de detección de intrusos y ventanas de seguridad (si estas áreas se encuentran en primeros pisos)?	SI	NO	
			¿Las áreas claves son convenientemente localizadas y protegidas para reducir los riesgos de amenazas y de peligros ambientales, y para reducir las oportunidades para el acceso no autorizado?	SI	NO	
			¿Cuándo es necesario el acceso de un visitante se registre el acceso de este a las áreas sensibles, se revoca el acceso al finalizar su visita y es constantemente supervisado?	SI	NO	
			¿Es apropiado el equipo contra incendios localizado en todas las áreas?	SI	SI	
			¿Se tiene prohibido comer, tomar o fumar en las áreas de procesamiento de información?	SI	NO	
			¿Están las instalaciones para el tratamiento de la información protegidas contra apagones (utilizando sistemas de alimentación interrumpidas o plantas eléctricas) u otras anomalías eléctricas (utilizando estabilizadores)?	SI	NO	Se tiene reguladores en todos los equipos. Sólo el servidor tienen UPS.
			¿Es adecuado el abastecimiento de agua y es estable para apoyar sistemas de aire acondicionado, manejo de la humedad y del fuego?	SI	SI	
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
		Administración de instalaciones.	¿Existe una política formal en la organización donde se asegure el buen uso de instalaciones móviles (Ejemplo: *palmtops,* computadoras portátiles, teléfonos móviles, redes inalámbricas)?	SI	NO	
			¿El mantenimiento a los equipos de cómputo es realizado por personal autorizado, se ejecuta en intervalos de tiempos recomendados y se registra los daños encontrados?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
Seguimiento de problemas y *logs* de Auditoría	Se identifican e implementan los registros y herramientas que permitan realizar las labores propias de auditoría.	Registros de elementos para auditoría	¿Los sistemas de información están supervisados y los eventos de seguridad de la información se registran?	SI	SI	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Toda la actividad de monitoreo y de auditoría cumplen con requisitos legales y mejores practicas establecidas, tales como IIA, ISO y/o COBIT?	SI	NO	
			¿Los registros de la auditoría se producen y se conservan por un período de tiempo convenido?	SI	NO	
			¿Los registros de monitoreo de actividades se protegen contra la modificación y el acceso no autorizados, incluyendo administradores de sistemas con privilegios de gran alcance?	SI	SI	
			¿Los registros son revisados sobre una base regular por un revisor independiente?	SI	NO	Sólo se revisan registros más operativos
			¿Los errores de sistema, las fallas de acceso al sistema y los "*logs*" son revisados regularmente, y se toman acciones correctivas?	SI	SI	Se revisan los logs sólo cuando hay inconsistencias
			¿Los relojes del sistema se sincronizan con una fuente exacta de tiempo para controlar los registros de auditoría?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
CUMPLIMIENTO DEL NIIVEL	**NO CUMPLE EL NIVEL**					

NIVEL 4

La organización realiza auditorías al sistema de gestión de seguridad de la información y recolecta métricas para establecer la efectividad de los controles						
PROCESO	**META**	**PRÁCTICA**	**CRITERIO**	**APLICA**	**RESPUESTA**	**OBSERVACIÓN**
Implementación y evaluación del plan de continuidad	La organización trabaja continuamente en la conservación de la seguridad de la información a través de revisiones y modificaciones constantes a los planes de continuidad del negocio.	Revisión y actualización del plan de continuidad.	¿El plan de continuidad se revisa cada 6-9 meses?	SI	SI	
			¿El proceso de continuidad del negocio incluye la revisión y actualización del plan para asegurar la eficacia continua?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
Monitoreo del Proceso.	La organización evalúa el correcto funcionamiento de los procesos de TI.	Implementación de indicadores para medir los procesos.	¿Se cuenta con reportes desarrollados a partir de los indicadores de medición donde se presenta el desempeño de los procesos de TI?	SI	NO	
			¿Se realizan encuestas para evaluar la satisfacción de los clientes acerca de los procesos de TI?	SI	NO	
			¿Se registra el tiempo entre la notificación de una deficiencia y el inicio de su accion correctiva?	SI	SI	Se registra la fecha, pero no se hace nada con ellos
			¿Se tiene un indicador acerca del total de procesos monitoreados en la organización?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
Administración de controles.	La organización trabaja continuamente en la conservación de la seguridad de la información a través de revisiones continuas a los controles implementados.	Administración de accesos.	¿Hay un proceso de autorización para conceder privilegios y se mantiene un *log* de todos los privilegios asignado?	SI	NO	
			¿Las autorizaciones de acceso al los sistemas se revisan en intervalos regulares?	SI	NO	Solo se realizan en los cambios grandes de personal
			¿Las capacidades de acceso de usuarios a los sistemas son revisadas cada 6-8 meses?	SI	SI	
			¿Las autorizaciones para los privilegios de acceso son revisadas cada 2-6 meses?	SI	SI	
			¿Los cambios de control de acceso para las cuentas privilegiadas se registran?	SI	NO	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿La asignación de privilegios se comprueba en intervalos de tiempo regulares?	SI	NO	
			¿Las guías de las buenas prácticas determinadas por la gerencia son comunicadas a los usuarios según sus responsabilidades en el aseguramiento, particularmente en la asignación y uso de contraseñas, la protección del equipo desatendido, y la importancia de una política de "escritorio limpio"?	SI	SI	
			¿Las cuentas de los usuarios que cambian de funciones o son retirados de la organización, son removidas inmediatamente?	SI	NO	Se dejan ocho días.
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
		Administración de contraseñas.	¿Los sistemas validan que las contraseñas se cambien regularmente por otras cuya longitud no sea inferior a seis caracteres y no haya sido recientemente utilizada?	SI	NO	
			¿Al momento en que un usuario recibe su contraseña, el sistema obliga al inmediato cambio de esta luego de la primera conexión?	SI	SI	
			¿Las contraseñas son confidenciales e individuales (únicas para cada usuario)?	SI	SI	
			¿Cuándo se escribe la contraseña en los sistemas esta no se exhibe en pantalla y tiene cifrado sostenido?	SI	SI	
			¿Se sugiere a los usuarios, para el mantenimiento de las contraseñas, al menos tres de los siguientes consejos: Nunca escriba su contraseña. (Memorícela), no cree una contraseña de fácil adivinación, nunca almacene la contraseña como una macro, nunca comparta la contraseña o no use palabras de diccionario?	SI	SI	
		CUMPLIMIENTO DE PRÁCTICA:	CUMPLE			
		Control de los datos para pruebas.	¿Existen controles para el acceso a los sistemas de prueba de datos?	NO		
			¿Se aplican los mismos controles de accesos tanto a los datos de prueba como a los reales?	NO		

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
			¿Se tiene diferentes autorizaciones de acceso para los datos de prueba y para los datos reales?	NO		
			¿Son borrados los datos de pruebas luego de realizadas estas?	NO		
			¿Se guardan registros de la utilización de datos reales para la realización de pruebas?	NO		
		CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE O NO APLICA			
		Administración de herramientas para garantizar la confiabilidad en las trasmisiones de información.	¿Existe un sistema de administración de claves conveniente en la organización, basado sobre un sistema de estándares, procedimientos y de métodos seguros?	SI	NO	
			¿Se toma el cuidado apropiado para proteger la integridad y la confidencialidad de las llaves privadas cuando se emplean firmas digitales?	SI	NO	
			¿Se han dado todas las consideraciones correspondientes a los aspectos legislativos sobre el estado y uso de firmas digitales?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE			
Monitoreo del control interno	La organización desarrolla y fortalece programas de auditoria para mantener el control interno dentro de esta.	Definición de la auditoria dentro de la organización.	¿Las auditorías de los sistemas operacionales se planean, se convienen y se realizan de una manera controlada (que reduce al mínimo el riesgo de la interrupción del proceso del negocio)?	SI	SI	
			¿La política de auditoría de los sistemas de información esta acorde con los requisitos de la gerencia?	SI	SI	
			¿La política de auditoría de los sistemas de información restringe el acceso al auditor a solo lectura para el software y los datos, y se monitorea y registra sus accesos?	SI	NO	
			¿La política de auditoría de los sistemas de información determina la disponibilidad de los recursos para realizar dicha actividad?	SI	SI	
			¿Los procedimientos de auditoria están debidamente documentados?	SI	SI	
			¿Dentro de la política de auditoría de los sistemas de información existen acuerdos para ejecuciones especiales?	SI	NO	El proceso en la organización se ejecuta diario
			¿Se incluye los servicios de auditores independientes o externos dentro de la política de auditoría de los sistemas de información?	SI	NO	

PROCESO	META	PRÁCTICA	CRITERIO	APLICA
			¿Los hallazgos encontrados en los procedimientos de revisión son reportados a un nivel adecuado de la organización, esto es, se informa a la persona encargada de la función que tuvo el inconveniente y a su jefe inmediato?	SI
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRÁCTICA:	NO CUMPLE	
CUMPLIMIENTO DEL NIIVEL:	**NO CUMPLE EL NIVEL**			

NIVEL 5

Existe una mejora continua del sistema de gestión de seguridad de la información, basada en la realimentación cuantitativa y cualitativa de las auditorias al sistema de seguridad de la información.						
PROCESO	**META**	**PRÁCTICA**	**CRITERIO**	**APLICA**	**RESPUESTA**	**OBSERVACIÓN**
Afinamiento y mantenimiento del plan de continuidad	Mantener el plan de continuidad lo más actualizado posible frentes a los cambios significativos que se den en la organización y en su entorno.	Mejoramiento continúo.	¿Los cambios significativos internos (en los sistemas o aplicaciones, el personal, la ubicación física o en los procesos claves del negocio) conllevan una revisión del plan de continuidad del negocio?	SI	SI	
			¿Los cambios externos (contratos convenidos con otras organizaciones, legislativos o de proveedores) conllevan una revisión del plan de continuidad del negocio?	SI	NO	
			¿El plan de continuidad es revisado y actualizado cada 6-8 meses?	SI	SI	
			Si el plan de continuidad se ejecutó ante alguna eventualidad, ¿se realiza alguna retroalimentación para evaluar los puntos en que se pueda mejorar?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
Evaluar lo Adecuado del Control Interno.	Asegurar el cumplimiento de los objetivos del control interno establecidos para los procesos.	Revisión del control interno	¿La gerencia revisa los puntos vulnerables y problemas de seguridad reportados por el monitoreo continuo de los controles internos?	SI	SI	
			¿La gerencia tiene identificas las fuentes que suministran la información necesaria para la toma de decisiones acerca de los eventos de control interno?	SI	SI	
			¿Se mide el tiempo de respuesta entre la deficiencia del control interno y su notificación a la alta gerencia?	SI	NO	Sin embargo por cultura se debe mantener informado
			¿Se tiene establecido reportes del cumplimiento del control interno?	SI	SI	
			¿Se realiza auditorias externas de forma periódica?	SI	SI	
			¿Son los informes de las auditorias externas revisados por la alta gerencia y se toman las medidas correspondientes sobre sus recomendaciones?	SI	SI	
CUMPLIMIENTO DEL PROCESO:	CUMPLE	CUMPLIMIENTO DE PRACTICA:	CUMPLE			

PROCESO	META	PRÁCTICA	CRITERIO	APLICA	RESPUESTA	OBSERVACIÓN
Reportes Gerenciales del monitoreo del proceso.	Mantener informada a la alta gerencia acerca del cumplimiento de los objetivos pactados y se toma decisiones en base a estos.	Informar a la alta gerencia del cumplimiento de metas establecidas.	¿Existen reportes gerenciales que indiquen el avance de la organización con respecto al logro de los objetivos planeados, la obtención de productos, el cumplimiento de los objetivos planteados y la mitigación de riesgos?	SI	SI	
			¿Se guía los planes de acción de la alta gerencia con respecto a la seguridad de la información con base a los reportes existentes?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
Reportes de violación y actividades de seguridad.	Monitorear constantemente los eventos que ponen en riesgo la información.	Reportar actividades de seguridad.	¿Las violaciones y las actividades de seguridad son registradas, reportadas y escaladas apropiadamente, por parte de los encargados de la administración de los servicios de información, en forma regular, para de esta manera identificar y resolver actividades no autorizadas?	SI	NO	
			¿Se analizan los reportes de violaciones para identificar puntos críticos que puedan ser resueltos por la gerencia de TI?	SI	NO	
CUMPLIMIENTO DEL PROCESO:	NO CUMPLE	CUMPLIMIENTO DE PRACTICA:	NO CUMPLE			
CUMPLIMIENTO DEL NIIVEL:	**NO CUMPLE EL NIVEL**					

CONCLUSIONES

- La fusión entre el modelo CMMI, la norma ISO 17799 y la herramienta CoBit permiten desarrollar un modelo más exhaustivo que permite ajustarse a la organización a evaluar, esto debido a la generalidad y madurez de sus procesos y al amplio alcance que tienen cada una de estas herramientas y modelos.

- La distribución del modelo en seis niveles de madurez permite realizar una clasificación más exacta del estado actual de seguridad de la información en la organización y presentar sus deficiencias a mejorar para lograr un nivel que constituya mayor seguridad, lo que conlleve a una mayor credibilidad y competitividad de la organización internamente y en su entorno.

- Para obtener el máximo beneficio del modelo aquí propuesto, es necesario conocer e indagar, antes de comenzar a aplicar la evaluación, acerca de la organización, su estructura, entono y sector al que pertenece, haciendo especial énfasis en el área de TI, ya que con esto se contextualiza y se puede definir qué aspectos del modelo aplicarían.

- El trabajo de campo permitió organizar de una manera estructurada y referenciada los criterios de evaluación que se tenían previamente identificados y clasificados según su relevancia, para lograr de esta manera conseguir evaluar lo realmente necesario en cada uno de los niveles del modelo propuesto.

- El desarrollo de un esquema de evaluación como el propuesto en este proyecto permite obtener unos resultados cuantitativos, ubicando la organización en un nivel determinado; sin embargo, el mayor beneficio que presta el modelo es presentar una descripción detallada de las debilidades encontradas durante la evaluación y esto es lo que realmente genera valor al momento de realizar planes de acción.

- La madurez de los proceso a través de la evaluación ofrece a las organizaciones mecanismos que permiten no solo implementar controles frente a los riesgos identificados en los niveles iniciales, sino que además promueve evaluaciones

continuas que permitan actualizar estos controles frente a nuevas amenazas externas e internas.

- Como base fundamental para el éxito del modelo es necesario realizar una adecuada clasificación de los activos físicos y lógicos, y una evaluación de los riesgos a los que está expuesta la organización para cada uno de los activos identificados.

- La ejecución de este modelo en organizaciones que pretenden obtener la certificación de calidad puede ser de gran ayuda ya que permite identificar *gaps* y fallas en sus sistemas de control y procesos críticos de negocios.

- A pesar de que el modelo de madurez para la seguridad de la información propuesto en este proyecto es solo el comienzo de un amplio camino de aprendizaje e investigación, la elaboración de éste nos permitió tener un conocimiento más amplio acerca de las necesidades de las organizaciones sobre la seguridad de la información, las mejores prácticas que se deben llevar a cabo para garantizar la integridad, disponibilidad y confidencialidad de la información, y nos motivo a desarrollar la inventiva, la indagación y fortalecer el trabajo en equipo.

- Debido a que la empresa Reimpex S.A se encuentra actualmente en una etapa de certificación ISO 9001 la elaboración del trabajo de campo en dicha empresa le permitió identificar áreas de oportunidad de mejora que deberían ser analizadas y corregidas durante el proceso de certificación.

RECOMENDACIONES

- Como trabajo futuro se sugiere al grupo de investigación interesado en utilizar el modelo de seguridad aquí propuesto, se evalúe la posibilidad de actualizar el modelo bajo la versión 4.0 de CoBit y la norma ISO 27001, publicadas el 16 de diciembre de 2006 y Abril de 2007 respectivamente. Además, tener en cuenta la norma internacional ISO/IEC 20000, enfocada en la gestión de servicios de TI (Tecnologías de Información) como complemento a esta evaluación y la norma ISM3 (*Information Security Management Maturity Model*) que sirve para fortalecer la gestión de los sistemas de información de las organizaciones que utilicen estándares como CoBiT, ITIL, CMMI e ISO17799.

- Realizar trabajos de campo en organización de mayor tamaño y de distintos sectores a la realizada en este proyecto, para identificar así el comportamiento del modelo en distintas empresas y así decidir la viabilidad en estandarizar el modelo o adaptarlo para que sea más flexibles.

- La seguridad de la información no es tema que solo le incumbe a la gerencia de TI, sino que es factor que se debe implementar en toda la organización, comenzando por la alta gerencia y proyectándose a través de toda la organización de tal manera que todas las personas que hagan parte de esta incorporen la cultura de control.

- Al momento de realizar la evaluación es recomendable validar los criterios con las personas encargadas, solicitar la evidencia necesaria para dar fe del cumplimiento de estos y confrontar la información con los niveles superiores de la organización, esto para garantizar el correcto funcionamiento de los modelos.

GLOSARIO

- **Ad-hoc**: Procesos no estandarizado que se realizan por costumbre.

- **Batch:** Es un archivo de procesamiento por lotes.

- **Criptografía:** Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.[18]

- **EDI (*Electronic Document Interchange)*:** Es un estándar mundial de comercio electrónico que indica los documentos o transacciones electrónicas globales que una organización puede intercambiar con sus clientes, proveedores, entre otros.

- **Escritorio Limpio:** Práctica que recomienda mantener el escritorio lo más limpio y ordenado posible.

- **Firewall:** Es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

- **Firma Digital:** Las firmas digitales son una forma de verificar que un mensaje de correo electrónico es realmente de la persona que supuestamente lo ha enviado, y que no ha sido alterado.[19]

- **Gaps:** Brechas o disfunciones.

- **Gateways:** Es una puerta de enlace que sirve de punto de acceso a otra red.[20]

[18] *es.wikipedia.org/wiki*
[19] *www.clcert.cl*
[20] *es.wikipedia.org/wiki*

- **Hilatura:** Proceso de formación de un hilo redondo, lleno, de una longitud determinada, constituido por un número mayor o menor de fibras colocadas paralelas entre sí por medio de torsión.

- **Honeypots**: Software o conjunto de computadores cuya intención es atraer a *crackers* o *spammers*, simulando ser sistemas vulnerables o débiles a los ataques.[21]

- **Honeynet:** Tipo especial de *Honeypots* de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes.[22]

- **In house:** Desarrollos en tecnología que la misma empresa se encarga, por parte de un área ya constituida dentro de ella.

- **ISA (*Internet Security and Acceleration)*:** Tecnología que ayuda a proteger las conexiones en Internet.

- **Log:** Archivo que registra movimientos y actividades de un determinado programa.[23]

- **Rack:** Gabinete destinado a alojar equipamiento electrónico, informático y de comunicaciones.[24]

- **Screen Display**: Gráficos o imágenes en pantalla.

- **Swicthes:** Dispositivo electrónico de interconexión para el intercambio de redes de computadoras.[25]

[17,18] *es.wikipedia.org/wiki/Honeypot*
[23] *www.helpy.com.ar/adsl/glosario.htm*
[24] *es.wikipedia.org/wiki/Rack*
[25] *es.wikipedia.org/wiki/Switch*

- **Outsoursing:** Proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

- **Palmtops:** PDA´s o computadoras de mano.

- **Xfers**: Mecanismo de sincronización que permite las transferencias electrónicas de información**.**

- **Time-Out:** Función que inactiva la sesión del usuario luego de transcurrido un periodo de tiempo sin utilizar el sistema.

- **Testing:** Escaneo de puertos con accesos a Internet para detectar alguna falla que permita prevenir el robo de información.

BIBLIOGRAFÍA

- 3º Congreso Iberoamericano de Seguridad Informática CIBSI 2005, Universidad Técnica Federico Santa María. Valparaíso, Chile.

- Barrientos A. Andrea Marcela, Aleiza C. Karen Alexandra,INTEGRACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON UN SISTEMA DE GESTIÓN DE LA CALIDAD, Proyecto de Grado, Universidad EAFIT, 2005.

- CALIO TECNOLOGIES. Software de conformidad BS7799 / UNE71502 / ISO17799 en español [En línea] URL:<http://www.callio.com.es> (Consulta: 05 de Febrero, 2006).

- CISA (Certified Information Systems Auditor), CISA, 2003.

- COBIT, Objetivos de Control, Tercera Edición, año 2000, Comité directivo de Cobit, IT Governance Institute.

- CRUZ, Daniel. ISO 17799: La gestión de la seguridad [En línea]. (Barcelona, España). URL <http://www.virusprot.com/Art41.htm>. (Consulta: Agosto, 2006)

- Estratega-Consultoría estratégica en TI [En Línea].(Argentina). URL:<http://e-stratega.com.ar/cobit.htm>. (Consulta: 14 de Abril, 2007)

- Indicadores de Gestión para la Función de Tecnología de Información (TI) [En línea](España).URL<http://www.pc-news.com> (Consulta: Enero 20, 2007).

- INSTITUTO ARGENTINO DE NORMALIZACIÓN - "ESQUEMA 1 DE NORMA IRAM-ISO IEC 17799.Código de práctica para la administración de la seguridad de la información" Año 2002.

- International Standard ISO/IEC 17799 (2000). Information technology - Code of practice for information security management.

- ISO17799, ISO 27000 and Computer Security News [En línea] URL:<http://www.computersecuritynow.com> (Consulta: 05 de Febrero, 2006).

- ISO27000.es, ISO 27000 [En línea]. (España). URL <http://www.iso27000. es/doc_iso27000_all.htm>(Consulta: Marzo 20, 2007).

- ISO- Internacional Organization for Standarization [En línea] URL:<www.iso.org> (Consulta: 05 de Febrero, 2006).

- La COBIT y la organización del area de informatica [En Línea] URL<http://msaffirio.wordpress.com> (Consulta: 14 de Abril, 2007).

- PÉREZ, Mario. XML / EDI en el comercio electrónico. [En línea]. (México D.F, México). URL <http://www.monografias.com/trabajos25/xml-edi/xml-edi. shtml#qesedi>. (Consulta: Agosto, 2006).

- Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance. [En línea]. URL <http://www.riskworld.net> (Consulta: Mayo 19, 2006).

- SSE-CMM System Secirity Engineering - Capability Maturity Model [En línea] URL:<http://www.sse-cmm.org/index.html> (Consulta: 05 de Febrero, 2006).

- The ISO 17799 / ISO17799 Information Directory [En línea] URL:<http://www.iso17799software.com> (Consulta: 05 de Febrero, 2006).

- UNIVERSIDAD DE LOS ANDES. Administración de la seguridad Informática (ISIS 4408) [En línea] URL<http://sistemas.uniandes.edu.co/manager.php?id=718> (Consulta: 05 de Febrero, 2006)

- Wikipedia, la enciclpedia libre [En línea] URL <http://es.wikipedia.org/wiki> (Consulta: 14 de Abril,2007).