ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE POSGRADO EN CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO "SOPORTE AL USUARIO" BAJO LA NORMA ISO/IEC 27001 EN LA EMPRESA COPCIL CONSULTORA PROFESIONAL CIA LTDA.

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA EMPRESARIAL

ADRIANA DEL CARMEN SÁNCHEZ YANEZ

DIRECTOR: ING. XAVIER CAMACHO, MBA

Quito, Marzo de 2007

REFERENCIAS BIBLIOGRAFICAS

ALVÁREZ Gonzalo, PEREZ Pedro, Seguridad Informática para Empresas y Particulares, Mc Graw Hill y Panda, I edición, 2004.

FIRTMAN Sebastián, Seguridad Informática, Las amenazas y vulnerabilidades mas peligrosas al desnudo, Manuales USERS, MP Ediciones, Argentina, Buenos aires, 2005.

CLAPAM, ALEXANDER Alberto, PhD. Cómo implantar un sistema de gestión de seguridad de información, 2006

Information Security Governance: Guidance for Boards of Directors and Executive Management. IT Governance Institute.

MICROSOFT, Actualización Gerencial, Publicación Bimensual

FDEZ Eduardo, MOYA Roberto, PIANTTINI Mario, Seguridad de las Tecnologías de Información, AENOR, 2003

BURCH G. John, GRUDNITSKI Gary. Diseño de Sistemas de Información Teoría y Práctica, Noriega editores, México 1996.

COBB Stephen, Manual de Seguridad para PC y redes locales, 1994

ICONTEC, Norma ICONTEC ISO 9004, Gestión de la Calidad y elementos del sistema de calidad, Lineamientos.

ISO/IEC 17799-1:2005

ISO/IEC 27001:2005

INSTITUTO ECUATORIANO DE NORMALIZACIÓN, Norma Técnica Ecuatoriana, Sistema de Gestión de la Calidad, NTE INEN-ISO 9001:2001

UMBERTO ECO, Como hacer una Tesis, Gedisa, Barcelona 1998

KOONTZ – WEIHRICH. Administración, una perspectiva Global. McGraw- Hill. México. 1998.

PORTER, Michael E. *Ventaja Competitiva.* Compañía Editorial Continental. México. 1996.

STONER JAMES, WANKEL CHARLES, Administración, Tercera Edición, Phh Prentice Hall, México.

VON BERTALANFFY, LUDWIG. General Systems Theory. Nueva York. 1968.

DIRECCIONES INTERNET:

1. www.isaca.org/cobit.htm
2. www.csi.map.es/csi/pgm5m20.htm
3. http://scrc.nist.gov/publications/nistpubs/800-12/
4. www.iso27000.es

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por la Ing. Adriana del Carmen Sánchez Yánez, bajo mi supervisión.

Ing. Xavier Camacho, MBA.
DIRECTOR DE TESIS

DECLARACION

Yo, Adriana del Carmen Sánchez Yánez declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____

Adriana Sánchez Yánez

AGRADECIMIENTOS

A la Escuela Politécnica Nacional, a todos quienes conforman la carrera de Maestría en Gerencia Empresarial, por acogerme en sus aulas, en forma muy especial al Ing. Xavier Camacho MBA, quien con su conocimiento y experiencia supo guiarme durante el desarrollo de esta investigación y al grupo de profesores que trabajaron en la revisión de este documento.

A Copcil Consultora Profesional por su apertura y apoyo para cumplir los objetivos de esta investigación.

DEDICATORIA

A mi Dios por la fortaleza

A mi esposo por su amor y apoyo incondicional

A mis hijos Jaime Luis y Gustavo por su amor y paciencia

A mis padres por la formación

son quienes han hecho posible el finalizar esta nueva meta

Adriana

LISTA DE FIGURAS

RESUMEN

El presente trabajo de investigación: Diseño de un Sistema de Gestión de Seguridad de la Información para el proceso “Soporte al usuario” bajo la norma ISO/IEC 27001 en la empresa Copcil Consultora Profesional Cía. Ltda., busca establecer un programa comprensible que asegure la confidencialidad, integridad y disponibilidad de la información clave de la empresa desarrollado en base a los requerimientos de los objetivos de control y controles definidos en el anexo A de la norma ISO/IEC 27001:2005, que permita a la compañía protegerse de un amplio espectro de amenazas, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio.

En el capítulo I se expone una introducción a conceptos sobre seguridad de la información, la necesidad de información en la actualidad, y una breve reseña de sobre las normas ISO que dirigen el diseño del sistema de gestión de la seguridad de la información (SGSI).

Para el desarrollo del presente trabajo es necesario: el conocimiento de la infraestructura de la empresa y el diseño del proceso Soporte al usuario, que se encuentran documentados en el capítulo II.

En el capítulo III, se realiza un análisis y conocimiento de la naturaleza y dinámica de las normas ISO involucradas, como de los objetivos de control y controles establecidos para el desarrollo de la documentación del sistema de gestión de la seguridad de la información, así como de la documentación requerida para establecer el SGSI.

En el capítulo IV se desarrolla el diseño del SGSI de acuerdo a lo establecido en la norma ISO/IEC 27001:2005 el cual contiene: la definición de la política de seguridad, el análisis de riesgo, el enunciado de aplicabilidad, el manual de seguridad y manual de procedimientos.

PRESENTACION

La información puede existir de muchas formas, puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o electrónicamente, ilustrada en películas, o hablada en conversaciones. En el ambiente competitivo de hoy en los negocios, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas o externas, accidentales o maliciosas, además con el incremento del uso de nuevas tecnologías para almacenar, transmitir y recobrar información, se abre a un mayor número y tipos de amenazas.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un Sistema de Gestión de la Seguridad de la Información (SGSI), que tiene como propósito garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías de información.

Los SGSI abarcan a personas, procesos y tecnologías de la información y es el concepto sobre el que se construye ISO 27001.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta la seguridad de la información.

CAPITULO 1

INTRODUCCION

1.1 GENERALIDADES

"La seguridad no se compra, se gestiona".
"La seguridad no es un producto sino un proceso"

BRUCE SCHNEIER

La informática se está extendiendo a todas las actividades profesionales y humanas, un ejemplo de su importancia se puede señalar, en la afirmación del reglamento 460/2004 de la Comunidad Europea, "… las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y de electricidad. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez a la sociedad[1]"

La informática ha pasado a formar parte de la actividad cotidiana de empresas y particulares. Los computadores almacenan información, la procesan y la transmiten a través de redes, abriendo nuevas posibilidades de ocio y de negocio. Cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

La seguridad no es una disciplina de todo o nada, no existen sistemas 100% seguros. Cotidianamente se realizan innumerables acciones expuestas a diferentes riesgos, la seguridad gira en torno a la gestión del riesgo. Por que aunque sea de manera inconsciente, se realiza un sencillo análisis de riesgos y decidimos seguir adelante o no.

[1] Álvarez Gonzalo, Seguridad de la informática para empresas y particulares, primera edición, 2004, Pág. 2

La información es hoy en día uno de los activos más importantes de las organizaciones y como tal requiere de una protección adecuada. La seguridad de la información protege a ésta de un amplio espectro de amenazas, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio.

La información puede existir de muchas formas, puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o electrónicamente, ilustrada en películas, o hablada en conversaciones. En el ambiente competitivo de hoy en los negocios, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas o externas, accidentales o maliciosas. Con el incremento del uso de nuevas tecnologías para almacenar, transmitir y recobrar información, se abre a un mayor número y tipos de amenazas.

Los Sistemas de Gestión de la Seguridad de la Información SGSI (Information Security Management Systems, ISMS) son una manera sistemática de manejar la información sensible de una compañía para que permanezca protegida. Esto abarca a personas, procesos y tecnologías de la Información.

Se requiere establecer un programa comprensivo de seguridad de la información, dentro de todas las organizaciones, para asegurar la confidencialidad, integridad y disponibilidad de la información; entre los estándares mundialmente aceptados y disponibles actualmente, para cumplir con este requerimiento; existen:

ISO/IEC 17799:2005: Código de buenas prácticas para la Gestión de la seguridad de la información; e ISO/IEC 27001:2005 - BS 7799 Parte 2: Especificaciones relativas a la gestión de la seguridad de la información. Se trata de dos estándares que están muy relacionados pero que desempeñan papeles distintos. Así mientras que la primera parte se aplica en la etapa de NORMALIZACIÓN, la segunda parte es aplicable en la etapa de CERTIFICACIÓN. A través de una metodología estructurada, que contiene los criterios más aceptados y las mejores prácticas de la industria para lograr una efectiva administración y gestión de la

seguridad de información, que talvez aún no es considerado en el ámbito empresarial con la seriedad que merece, pero sin duda en corto plazo lo será.

1.2 RESEÑA HISTORICA DE COPCIL

COPCIL Consultora Profesional es una empresa privada que ofrece servicios de tercerización de la gestión financiera contable, tiene sus orígenes en el mes de febrero de 1978, en la ciudad de Quito y por objeto la prestación de servicios de asesoramiento y consultoría administrativa y empresarial para instituciones y empresas públicas, semipúblicas, mixtas y privadas; en las áreas de Contabilidad, Nómina, Administración de Inventarios, Tesorería, Facturación, Cobranzas.

Actualmente se encuentra ubicada en las ciudades de Quito y Guayaquil, y en su nómina constan 59 personas. En Quito esta domiciliada en la Av. Diego de Almagro N32-48 y Whimper y en la ciudad de Guayaquil domiciliada en Carchi 702 y Av. 9 de Octubre.

COPCIL es un empresa que se ha comprometido en realizar cambios de alto impacto para crear y mantener ventajas competitivas, tomando en cuenta que el entorno actual y futuro de la industria ecuatoriana, está condicionada por los factores: competencia, globalización, políticas de cambio, rentabilidad del crecimiento y servicio al cliente.

Copcil, además coordina y administra los servicios de Tecnologías de la Información y Comunicaciones, para dos empresas afines que se encuentran localizadas dentro del mismo edificio, con el objetivo de generar ahorros importantes a través de compartir recursos tecnológicos.

1.2.1 ESTRUCTURA DE LA ORGANIZACIÓN

La forma como está estructurada COPCIL Consultora Profesional se la puede apreciar en el organigrama funcional que se encuentra en el Anexo I.

COPCIL tiene dos departamentos para los servicios de tercerización que ofrece y estos son: Nómina y Contabilidad. Los departamentos de apoyo a la gestión de

servicio son: Soluciones de Tecnología (Informática), Marketing, Gestión Financiera, Recursos Humanos, y Asesoría Legal.

1.2.2 LOS SERVICIOS DE COPCIL

- *Contabilidad*.- Elaboración de estados financieros bajo normas locales, US GAAP, declaraciones tributarias, indicadores de gestión.
- *Tesorería, facturación, cobranzas*.- Gestión de cobranzas, pagos, control de cuentas bancarias, análisis financiero, etc.
- *Nómina*.- Manejo integral de la nómina del personal, declaración de impuestos, cumplimiento de obligaciones sociales, indicadores de gestión.
- *Administración de inventarios*.- Método de valuación, implantación de nuevos sistemas, planificación y control de inventarios.
- *Administración de activos fijos*.- Inventarios y conciliación, métodos de valuación, depreciaciones, revalorizaciones, implantación de base de datos, manual de procedimientos.

1.2.3 COMPETENCIA

La competencia son aquellas empresas que se dedican a realizar servicios de tercerización contable y de nómina. En la actualidad en el mercado existen muchas empresas dedicadas a ofrecer estos servicios, pero debido a que el mercado es grande y no solo una empresa puede abastecerlo, existe la posibilidad de compartirlo entre todos, lo importante es la diferenciación con que se realiza el trabajo buscando siempre la innovación y la satisfacción del cliente.

1.2.4 DIRECCIONAMIENTO ESTRATÉGICO DE LA EMPRESA

1.2.4.1 Misión

“Somos un grupo de profesionales que organiza, coordina y facilita la oferta de servicios de Consultoría y Asesoría Administrativa generando valor agregado para empresas públicas, semipúblicas y privadas, generando rentabilidad sostenible a la empresa y a sus accionistas”.

1.2.4.2 Visión

"Para el 2010 Copcil Consultora Profesional Cía. Ltda. será una de las 10 mejores empresas en ofrecer Consultoría y Asesoría Administrativa en el mercado y así lograr el crecimiento profesional y económico de nuestros empleados, accionistas y clientes, basándonos siempre en la confidencialidad, puntualidad, honestidad, excelencia, liderazgo y el trabajo en equipo".

1.2.4.3 Valores de COPCIL Consultora Profesional

Para COPCIL los principales valores bajo los cuales se orienta el trabajo de sus empleados son los siguientes:

"Trabajo en Equipo, que requiere:

Relacionamiento: Establecemos relaciones productivas y duraderas entre nosotros y con los clientes.

Respeto: Acogemos diversas culturas, comunidades y puntos de vista. Consideramos activamente las necesidades individuales, incluso la de calidad de vida.

Compartir: Estamos preparados para compartir conocimiento, experiencia, recursos y oportunidades.

Excelencia, a través de la:

Innovación: Desarrollamos soluciones creativas y las traducimos en acción.

Aprendizaje: Desarrollamos continuamente el conocimiento de nuestro negocio y las habilidades de cada persona.

Agilidad: Estamos alertas a los cambios y nos movemos rápidamente, con flexibilidad y decisión.

Liderazgo, que requiere:

Coraje: Somos osados. Capitalizamos oportunidades y asumimos responsabilidades.

Visión: Tenemos una visión amplia y objetiva, tenemos un sentido claro de dónde queremos llegar, lo que nos inspira y motiva.

Integridad: Somos confiables y honorables".

1.3 EL PROBLEMA

Todos los usuarios de informática, tanto del sector público o privado, poseen expectativas informales respecto a los ordenadores: esperan que al apretar el botón de encendido el computador conserve todos los datos tal como los dejaron el día anterior; cuando envían un mensaje de correo electrónico, esperan que llegue a su legítimo destinatario en un tiempo razonable sin perder los datos adjuntados; cuando acceden a la base de datos de nóminas, esperan que los sueldos y los nombres de los empleados sean auténticos y no hayan cambiado. Pero si no se toma ninguna medida de protección, la mayoría de las expectativas respecto a la informática se verán defraudadas, ya que la información está expuesta a innumerables amenazas, cada una con una probabilidad de ocurrencia y un riesgo asociado variables, como se puede ver en la figura 1.1, publicado por CERT (Computer Emergency Response Team), CERT es un centro experimentado de seguridad de Internet, localizado en EEUU en la universidad Carnegie Mellon, en el Instituto de Ingeniería de Software.

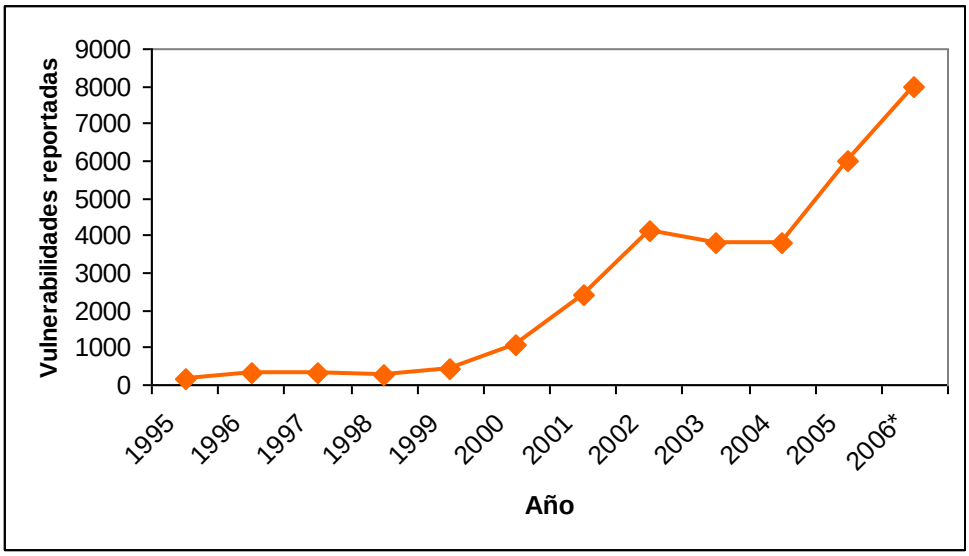


Fig. 1.1 Número de vulnerabilidades comunicadas al CERT (Computer Emergency Response Team)

Para COPCIL prescindir de prácticas adecuadas de seguridad informática puede tener un impacto enorme, dejarían de funcionar por completo si no estuvieran disponibles los servicios que proveen las TICs (Tecnologías de Información y Comunicaciones) o la información que éstas soportan; la compañía se vería

gravemente afectada si su información fuera modificada o accedida sin autorización de manera accidental o intencional por empleados o por terceros.

Hoy en día, debido a la gran dependencia tecnológica, la seguridad informática está directamente ligada a la supervivencia de esta compañía, y es de competencia tanto de la alta gerencia, como del área técnica la administración del riesgo para mantener en operación a la compañía.

1.4 OBJETIVOS DE LA INVESTIGACION

1.4.1 OBJETIVO GENERAL

Diseño de un Sistema de Gestión de la Seguridad de la Información empleando los requerimientos de la norma ISO/IEC 27001:2005 para el proceso “Soporte al usuario”, en la Empresa COPCIL CONSULTORA PROFESIONAL CIA LTDA, que le permitirá a COPCIL trabajar bajo normas internacionales de seguridad de la información.

1.4.2 OBJETIVOS ESPECÍFICOS

- Conocer los problemas más comunes de seguridad de la información en las empresas
- Realizar un levantamiento del proceso “Soporte al usuario” al cual se aplicará la norma.
- Diseñar el sistema de gestión para asegurar que el proceso “Soporte al Usuario” sea capaz de operar bajo un sistema que satisfaga los requisitos de las normas ISO/IEC 27001
- Desarrollar la documentación requerida por el Sistema de Gestión de Información de Seguridad de la Información

1.5 HIPÓTESIS DE TRABAJO

1.5.1 HIPÓTESIS GENERAL

La aplicación de la norma ISO/IEC 17799-1.2005 ayudará a que los servicios prestados por la empresa sean de calidad.

1.5.2 HIPÓTESIS ESPECÍFICAS

- La seguridad de la información dejo de ser una opción para convertirse en una obligación
- El diagnóstico de la situación actual es un punto de partida para el establecimiento del Sistema de Gestión de la Seguridad de la Información.
- La implantación, desarrollo y mantenimiento de un sistema de gestión de la información ayudará a dirigir y controlar las actividades que se realizan en la Empresa COPCIL.
- La documentación requerida por la norma ISO 17799-1:2005 ayuda en el mejoramiento de los servicios que presta la Empresa COPCIL CONSULTORA PROFESIONAL

1.6 LA SEGURIDAD DE LA INFORMACIÓN

1.6.1 LA INFORMACIÓN COMO ACTIVO[2]

1.6.1.1 Definición de la información

La información la componen datos que se han colocado en un contexto significativo y útil y se ha comunicado a un receptor, quien la utiliza para tomar decisiones. “La información implica la comunicación y recepción de inteligencia o conocimiento”.

Evalúa y notifica, sorprende y estimula, reduce la incertidumbre, revela alternativas adicionales o ayuda a eliminar las irrelevantes o pobres, e influye sobre otros individuos y estimula a la acción. Especialmente en los negocios, la información debe dar señales oportunas de aviso y anticipar el futuro. El gerente que sólo observa reportes históricos está tratando de ver adelante a través de un espejo retrovisor.

La información está compuesta de datos, imágenes, texto, documentos y voz, a menudo entrelazados en forma inextricable, pero siempre organizados en un contexto significativo. El término datos se empleará para abarcar a todos los

[2] Burch John, Grudnitski Gary, Diseño de Sistemas de información teoría y práctica, México 1996, Pág. 19

componentes de la información, pero es importante recordar que la información es algo más que simples números. En la figura 1.2 se muestra el ciclo que cumple la información.

Los datos se procesan mediante modelos para crear información; el receptor recibe la información y luego toma una decisión y actúa; esto genera otras acciones o eventos, que a su vez crean diversos datos dispersos, que se capturan y sirven como entrada; y el ciclo se vuelve a repetir.

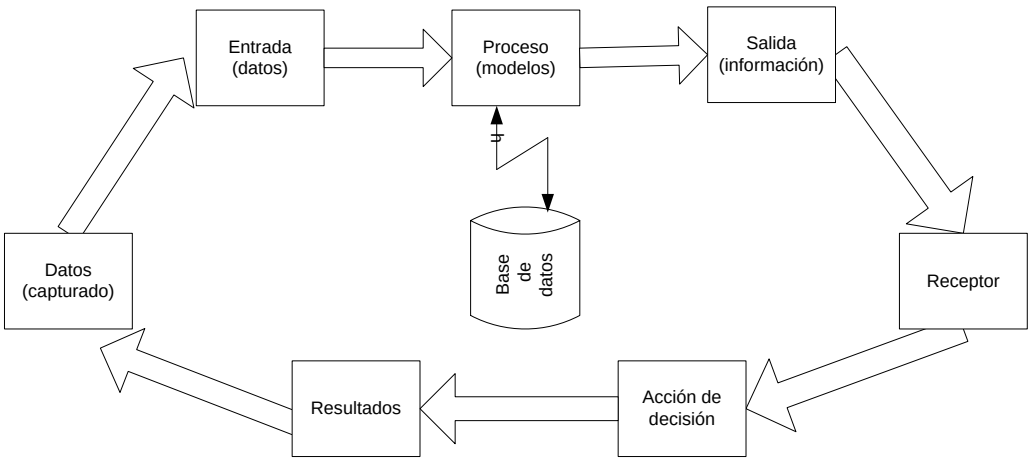


Fig. 1.2. El ciclo de la información

1.6.1.2 Historia de la necesidad de información

El presente es con frecuencia mucho más significativo cuando se tiene una mejor comprensión del pasado. A decir verdad, muchos de los historiadores consideran que una de las características principales de las civilizaciones progresistas es su habilidad para producir y utilizar la información de manera eficaz. Por ejemplo, en el valle de Mesopotamia florecieron civilizaciones en fechas tan lejanas como 4500 a.C. Un punto interesante es que estas civilizaciones mantenían registros bastante sofisticados en tabletas de arcilla de varias formas y tamaños. Estos dispositivos de almacenamiento proporcionaban una gran cantidad de información acerca de ingresos, desembolsos, inventarios, préstamos, compras, arrendamientos, formación y disolución de sociedades, y contratos.

Hace más de 500 años los incas de Sudamérica desarrollaron sistemas de información bastante completos con bases de datos y modelos de procesamiento

compuestos de miles de cuerdas con nudos denominadas quipus. Por ejemplo, los nudos en cuerdas colgantes representaban el número de personas en un poblado, sus deberes, la cantidad de grano en un almacén, transacciones comerciales, poesía, registros de batallas y otros eventos históricos. Un arreglo de nudos y diferentes colores proporcionaba una combinación de nemónicos, dígitos e información narrativa. Las personas que construían estos sistemas recibían el nombre de quipuamayus, precursores de los analistas de sistemas de estos días.

A mediados del siglo XVIII aumentaron las presiones para el procesamiento de datos. La Revolución Industrial sacó del hogar y del taller los medios básicos de producción y los puso en la fábrica. El desarrollo de los grandes fabricantes condujo al desarrollo de las industrias de servicios para la comercialización y transportación de los productos de los fabricantes. El creciente tamaño y complejidad de estas organizaciones hacía imposible que alguna persona obtuviera suficiente información para administrarla en forma efectiva sin recurrir a la ayuda del procesamiento de datos. Además, con el advenimiento de los grandes sistemas fabriles y las técnicas de producción masiva, la necesidad de bienes de capital más sofisticados requería de grandes inversiones y la necesidad de estos grandes capitales obligó a separar al inversionista (dueño) de la gerencia (administrador). Por una parte, la gerencia necesitaba mayor información para las decisiones internas, en tanto que los inversionistas, por otra parte, necesitaban información acerca de la organización y acerca del desempeño de la gerencia.

1.6.1.3 La necesidad de información en la actualidad

En el siglo XXI está creciendo la necesidad de producir más información, que esté disponible para un mayor número de usuarios. Los inversionistas de una empresa necesitan información acerca de su estado financiero y sus perspectivas futuras.

Los banqueros y los proveedores necesitan información para evaluar el desempeño y la solidez de un negocio, antes de proceder a un préstamo o concederle crédito. Las agencias del gobierno necesitan ver las actividades financieras y operativas para actos de impuestos y reglamentación. Los sindicatos están interesados en las utilidades de las organizaciones en las que trabajan sus

afiliados. Sin embargo, los individuos que están más involucrados con la información y dependen de ella son los que tienen a su cargo la responsabilidad de administrar y operar las organizaciones, es decir, la gerencia y los empleados; sus necesidades van desde el mantenimiento de las cuentas por pagar hasta la información estratégica para la adquisición de otra compañía. Como dijo un alto ejecutivo de Sears: “Cuando se intenta seguir la pista a tantas cosas como nosotros lo hacemos, la información oportuna y exacta es el recurso esencial para mantener las operaciones y ser competitivos”.

1.6.1.4 Atributos de la información

Muchas personas aún tienden a creer que la información son listados de computadora, otras afirman que los usuarios están sufriendo de una sobrecarga de información. Realmente están inundados por información, pero muchos usuarios carecen aún de información de calidad. Como se ilustra en la Figura 1.3, la calidad de la información descansa sólidamente sobre tres pilares: exactitud, oportunidad y relevancia; que constituyen los atributos claves de la información.

La *exactitud* significa que la información esté libre de errores. Significa que la información es clara y refleja adecuadamente el sentido de los datos en los que se basa. Transmite una imagen clara al receptor, lo cual puede requerir una presentación en forma gráfica en vez de tabular. La exactitud significa que la información está libre de tendencias o desviaciones.

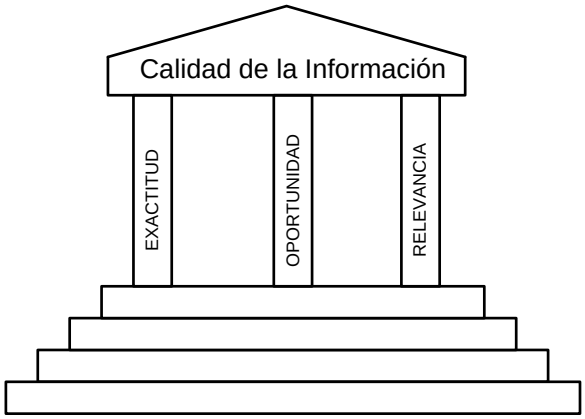


Fig. 1.3 Atributos de la calidad de la información

El hacer llegar la información a los receptores dentro del marco de tiempo necesario es otro atributo clave de la calidad de la información. Obviamente, por lo general es de poco valor el periódico de ayer, las variaciones con respecto al estándar que se reportan después de que pueda tomarse una acción correctiva, o la información sobre las existencias uno o dos días después de los hechos.

La *oportunidad* en la información significa simplemente que los receptores la puedan obtener cuando la necesitan.

La *relevancia* es el último atributo clave de la calidad de la información. En palabras sencillas, la información responde de manera específica al receptor sobre el ¿qué?, ¿por qué?, ¿dónde?, ¿cuándo?, ¿quién? y ¿cómo?. Además, lo que es información relevante para un receptor, no lo es necesariamente para otro.

1.6.1.5 El valor de la información y su seguridad

Día a día aumenta el potencial de sabotaje informático. Centenares de virus se renuevan, perfeccionan, multiplican con la finalidad de robar o acabar con la información en las redes informáticas. Existe la necesidad de incrementar políticas de seguridad y responsabilidades para el manejo de la información, aunque se multipliquen las medidas para la protección, los hackers y virus avanzan con mayor rapidez. Quienes protegen la información cada vez cuentan con menos tiempo para vacunar o parchar errores, de forma que se está luchando contra el crimen informático y contra el tiempo.

No obstante, y pese a que sí se debe reforzar las políticas de seguridad de sistematización, está claro que la mejor forma de prevenir catástrofes empresariales por la pérdida de información, es la educación.

Un sinónimo de defensa efectiva es el nivel de conocimiento que los usuarios tienen sobre la tecnología que manejan. La maquinaria, los transportes e incluso las personas, son sustituibles o están asegurados, pero sin la información comercial, contable, administrativa, etc., una empresa no tendría ningún valor. Es peor aún si esa información es perdida o publicada a su competencia y similares.

Por ello, las tecnologías de la información y comunicación (TIC) se han convertido en un elemento estructural para dar soporte a uno de los principales activos de una empresa: la información.

1.6.1.6 La información y la organización

Los componentes esenciales de una organización pueden verse en función del área de trabajo, la cultura, la base de sus activos y los interesados y afectados. Para que una organización funcione sin obstáculos, estos componentes deben estar orientados hacia los mismos objetivos y estar sincronizados entre sí. La información es el ingrediente clave que le permite a una organización lograr y mantener un estado de unidad y armonía. En la figura 1.4, se presentan los componentes principales de una organización.

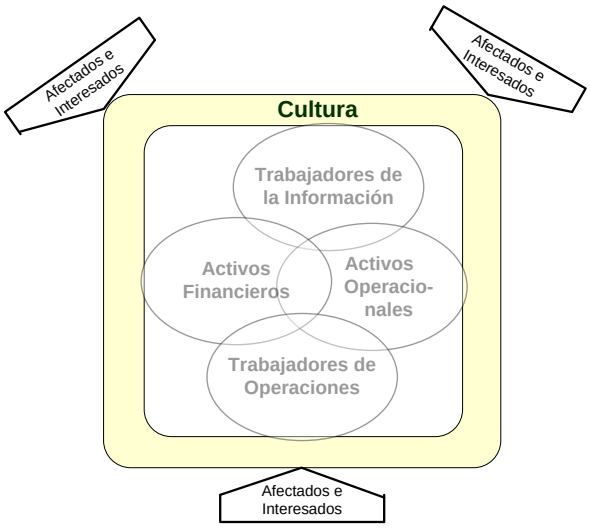


Fig. 1.4 Los componentes principales de una organización

1.6.1.6.1 El área de trabajo

La organización está formada por personas que se unen para lograr un objetivo común: crear y ofrecer un producto o servicio. Por ejemplo, un fabricante convierte materias primas en productos terminados, un banco proporciona servicios financieros y un hospital ofrece servicios médicos. El trabajo para lograr los objetivos de la organización se divide entre las personas de acuerdo con sus habilidades y los objetivos de sus tareas, y luego se unen para lograr una coordinación general. El trabajo incluye actividades físicas y mentales, y en algunos casos una combinación de ambas. Sin embargo, aquí se estudiará el área de trabajo desde el punto de vista de los trabajadores de operaciones,

quienes tienen una orientación física y los trabajadores de la información, quienes tienen una orientación mental.

1.6.1.6.2 Trabajadores de operaciones

Estos trabajadores están involucrados directamente con la fabricación y distribución de productos o la prestación de un servicio. En las compañías manufactureras, por ejemplo, los trabajadores de operaciones están involucrados en la conversión de materias primas en productos terminados. A medida que aumente la automatización en el área de trabajo de operaciones, aumentará la necesidad de información en esta área.

1.6.1.6.3 Trabajadores de la información

La mayoría de la fuerza laboral trabaja con información. Algunas estimaciones indican que más de la mitad de la fuerza laboral está involucrada con la información o con el procesamiento de la misma más del 90% del tiempo[3]. Incluso los trabajadores empleados directamente en las operaciones como los torneros, operadores de taladros, choferes o los trabajadores agrícolas están involucrados en funciones de información y la requieren como ayuda. Los contadores, empleados de oficinas, ingenieros, abogados, programadores de computadoras, analistas de sistemas, gerentes, físicos, bibliotecarios y auditores, todos ellos son trabajadores de la información.

La información es obviamente el ingrediente principal de su trabajo. La creación, procesamiento, distribución, interpretación y análisis de información es su trabajo o tarea. Manejan toda clase de mensajes, llamadas telefónicas y memos. Estudian reportes, preparan reportes, toman decisiones, actúan debido a las decisiones que se han tomado, dirigen o asisten a reuniones, e inician y dan seguimiento a las actividades.

Los trabajadores de la información se pueden dividir de manera general en tres amplias categorías: (1) usuarios primarios de la información, como los gerentes que utilizan la información para el control, planeación y toma de decisiones, (2)

[3] Burch John, Grudnitski Gary. Diseño de sistemas de información teoría y práctica, México 1996, Pág. 25

aquellos que a la vez son usuarios y proveedores de información, como los contadores, y (3) el personal de soporte de la información, como las secretarias, programadores, operadores de computadoras, especialistas en tecnología informática, administradores de base de datos y analistas de sistemas.

En la actualidad, la parte con mayor personal laboral en las organizaciones está en el área de los trabajadores de la información. Sin embargo, el equipo de capital para el respaldo de los trabajadores de operaciones supera en mucho al equipo de soporte para los trabajadores de la información, a pesar de la proliferación del trabajo rutinario de oficina (papeleo) y la necesidad de información. Son esenciales los sistemas de información que pueden eliminar los cuellos de botella en el papeleo y proporcionar un acceso rápido a la información para una diversidad de usuarios. No hay duda de que los gastos en tecnología informática para los trabajadores de la información aumentarán de manera significativa en el futuro.

1.6.1.7 La base del activo

La base del activo se puede definir en diversas formas. Por ejemplo, se podría decir que la base del activo de una organización la componen: las personas, el dinero, las máquinas, los materiales y los métodos. O bien, los activos se puede describir como tangibles (p. ej., planta y equipo) e intangibles (p. ej., patentes, derechos de autor y secretos comerciales). Esto simplemente muestra los activos financieros y operacionales. No obstante, en cualquier de estos caso se necesita información para el seguimiento de estos activos, para mostrar qué tan bien se están empleando o para señalar cómo se podrían emplear mejor. De hecho, la eficacia y la eficiencia en el empleo de los activos es uno de los factores clave del éxito de cualquier organización.

a) Los activos financieros son el efectivo o lo que se puede convertir fácilmente en efectivo. Estos activos proveen la “energía” de inversión de la organización. En las compañías no financieras, como las manufactureras, los activos financieros soportan las operaciones y proporcionan los medios con los cuales la organización puede crecer y prosperar. La información

requerida comprende también los presupuestos de capital y los análisis de inversión, la participación en el mercado, los pronósticos de ventas, etc.

En las instituciones financieras como las compañías de seguros y los bancos, el activo principal es el dinero. Por ejemplo, una compañía de seguros cobra las primas, invierte este dinero, y subsecuentemente paga dinero bajo la forma de reclamaciones, beneficios por fallecimiento o anualidades. La medición de qué tan bien se está utilizando este dinero y las utilidades de cada tipo de póliza de seguros son imperativas para el éxito de la compañía de seguros.

b) Los activos operacionales son todos los activos tangibles e intangibles requeridos para producir y distribuir un producto o un servicio. En una compañía manufacturera o constructora, estos activos incluyen a todo el inventario, los bienes raíces, la planta y el equipo, las patentes, etc. En las organizaciones de servicios, tanto lucrativas como no lucrativas, como los hoteles, restaurantes, bancos, hospitales, agencias de gobierno e instituciones educativas, la base del activo tiene relativamente poco inventario. Algunas organizaciones profesionales, como las firmas de contabilidad, ingeniería y de abogados, tienen bases de activo pequeñas y sencillas, ya que su activo principal es su personal profesional (aunque cualquier organización también podría decir que su activo principal es su gente). Sin embargo, como sucede en todas las organizaciones, los activos del personal no aparecen en la hoja del balance. No obstante, el flujo de información acerca de los “activos” en una organización profesional es tan importante como en las otras organizaciones, especialmente la información referente a la administración y la programación del tiempo, la correspondencia, la clasificación de documentos, las minutas de las juntas, diversos reportes y contratos, facturación y la evaluación del desempeño del personal.

Las diferentes organizaciones tienen diferentes necesidades respecto a ciertas clases de información, pero independientemente de su tipo o naturaleza, todas las organizaciones necesitan una información referente a sus activos. Por ejemplo,

todas ellas necesitan información contable básica, que incluye facturación, contabilidad de costos, nómina, cuentas por cobrar, cuentas por pagar, y varios reportes financieros y de auditoría. Todas necesitan información de comercialización; que incluya análisis de ventas de productos o servicios, investigación de mercados, pronósticos de ventas, perfiles competitivos y correspondencia. Ya sea que se incluya o no a los trabajadores en la base del activo, la organización necesita obviamente información sobre el personal; esto incluye los registros y prestaciones de los empleados, reportes de igualdad de oportunidades de empleo, inventario de conocimientos y capacidades, apertura de empleos, descripciones de puestos, manuales de capacitación y de políticas, y correspondencia.

La adquisición de activos incluye información como órdenes de compra, existencias de seguridad, cantidades pedidas, especificaciones, desempeño de los proveedores, solicitudes de cotización y correspondencia. Toda esta información es universal en todas las organizaciones y representa el mínimo requerido para una administración, control y empleo adecuados de los activos.

1.6.1.8 Valoración de los sistemas de computadoras

Determinar el valor de un sistema basado en una computadora, las tareas que realiza y la información que manipula para llevar a cabo dichas tareas es un trabajo complejo, así como las consecuencias de que dejen de funcionar. Para la determinación de esto se ha considerado que existen cuatro factores principales en el valor de cualquier sistema de computadora personal:

a) El equipo en sí mismo.
b) El software usado por el equipo para procesar información.
c) La información procesada.
d) La capacidad del sistema para continuar realizando el procesamiento.

1.6.1.8.1 El equipo

La mayoría de los equipos resultan fáciles de valorar. Podría saber sin dificultades lo que la empresa ha pagado por ellos. Podría asignar un valor a un equipo usando conceptos económicos habituales, como precio de compra, valor de sustitución, valor de depreciación y demás.

1.6.1.8.2 El software

El valor del software es un tema complicado. Generalmente se compra el derecho a usar el software, en vez del escaso material compuesto por discos y manuales, si alguien robará la copia del manual o el disco de sistema, bajo los contratos de licencia habituales, continua teniendo derecho a usarlos. Evidentemente, para que este derecho tenga un valor, necesitará demostrar que adquirido realmente el programa. En el caso del software escrito por el usuario, o desarrollado internamente, el tema del valor se complica increíblemente. Un programa muy específico para un ámbito o empresa puede tener poco valor para otros usuarios. Si pierde todas las copias del programa y quién lo ha desarrollado ya no trabaja, el programa podría llegar hacer de un valor incalculable.

1.6.1.8.3 La información procesada

Aunque el término "procesamiento de información" trae a la mente facturas, pedidos de clientes, listas de correo y demás, en algunas computadoras personales tiene un significado distinto. La información procesada incluye estimación de presupuestos, cartas, informes, propuestas, resúmenes y demás. Cualquier tipo de información manipulada por una computadora personal presenta varios aspectos:

- El valor para los usuarios.
- El valor para los demás.
- El valor negativo.
- El valor del acceso inmediato.

a) *El valor para los usuarios.* Si se pierde la última hoja de cálculo de estimación de costos para un proyecto competitivo. Volver a crear la hoja costará tiempo y esfuerzo. También podría experimentar una pérdida de credibilidad y confianza dentro de la empresa si la pérdida del archivo supone una rotura del esquema de planificación de presentación del proyecto. Esto demuestra el auténtico valor personal de la información para el usuario. Si el archivo perdido redunda en una operación fallida, queda claro el gran valor de los datos para el usuario y para la empresa.

b) *El valor para los demás*. En un supuesto en que el archivo que contiene la estimación de costos desaparece de la computadora personal para ir a manos de los competidores, que lo utilizan para coger el proyecto. Puede que ésta sea la demostración más evidente del valor de la información para los demás. Los datos tales como listas de clientes y estrategias de marketing entran en la misma categoría. Los competidores directos no son las únicas personas que pueden escamotear los datos del sistema informático. Si vende información en sí misma, es muy posible que haya personas capaces de pensar en cómo obtener gratis la información.

c) *El valor negativo*. La información que no tiene un valor directo para la empresa o sus competidores puede tener un valor negativo. Muchos pueden haber preparado alguna vez un texto jocoso en una computadora personal. Si éste está dedicado a un futuro jefe, descubrir el archivo del texto en la computadora del jefe actual puede resultar cuanto menos embarazoso. Ejemplos de información con un posible valor negativo podrían ser: comentarios sobre la seguridad de productos, evaluaciones de empleados, resultados de pruebas medioambientales y demás. De hecho, la mayoría de documentos internos que hablan negativamente de un organismo o persona tienen un posible valor negativo.

d) *El valor del acceso inmediato*. En un supuesto en que al llegar al trabajo por la mañana y la computadora personal no funciona como se espera. El archivo que necesita no está donde se lo había dejado. En una situación como ésta, descubre el valor del acceso inmediato. Puede que el archivo no se haya perdido para siempre, pero el acceso se retrasa, perdiendo tiempo y esfuerzo y causando un descenso de productividad.

1.6.1.8.4 Capacidad para seguir realizando el trabajo

Está íntimamente relacionada con el valor del acceso inmediato. A medida que las computadoras personales incrementan su capacidad de procesamiento se les asignan tareas cada vez más importantes. El uso de computadoras personales para tareas como el procesamiento de pedidos, reservas de clientes, gestión de

inventario y adquisición de datos implica que su papel sea crítico. El coste de una interrupción de funcionamiento del sistema puede ser considerable, en términos de pérdida de negocio y de imagen.

Por supuesto puede que las tareas realizadas con la computadora personal no resulten críticas para las ganancias y pérdidas de una empresa, pero pueden seguir siendo importantes para el usuario. Aunque está claro que la seguridad de las computadoras personales tiene que ver con que éstas sigan haciendo su trabajo, realizar afirmaciones precisas sobre el valor de las computadoras personales resulta difícil, por la capacidad que esta tiene. El método adecuado sería suponer que las computadoras personales con las cuales se realizan tareas, cuya importancia está clara para el usuario de ésta.

Podríamos buscar una respuesta teórica a la pregunta ¿qué hacen las computadoras personales? Por ejemplo, es cierto que se utilizan para procesar información. El factor crítico es la naturaleza de la información. Una computadora personal podría procesar información sobre las actividades de un avión simulado a medida que el usuario intenta derribar a un enemigo simulado.

El valor de esta información es limitado para personas distintas del usuario. Otra computadora personal podría procesar información sobre las actividades de un avión real, información de vital importancia para el piloto y los pasajeros. Lo que hace exactamente una computadora personal es menos importante que el hecho de que juega un papel valioso en un proceso.

1.6.1.9 Factores claves de las organizaciones

Los factores organizacionales juegan un papel principal en determinar la clase de información que se produce y la forma en que se comunica. Estos factores son la naturaleza, las categorías, el tamaño, la estructura y el estilo gerencial.

1.6.1.9.1 Naturaleza

La naturaleza propia o el propósito de una organización es uno de los factores principales que contribuyen a los requerimientos de información de la organización.

Todas las organizaciones son en cierta forma similares en áreas como la de nómina, cuentas por cobrar, cuentas por pagar y compras; sin embargo, incluso en estas áreas existen características como la orientación al mayoreo o al menudeo, el estar sindicalizadas o no, y la orientación hacia productos o servicios, que implican diferencias substanciales en los requerimientos de información.

En la mayoría de las organizaciones, la información y las actividades de procesamiento de la misma se consideran como funciones de apoyo al propósito principal de la organización. Sin embargo, para algunas organizaciones (p.ej., oficinas de crédito, bibliotecas y agencias gubernamentales) la función principal es la producción de información para otras organizaciones. Para otras el producto principal está estrechamente relacionado con el procesamiento de información (p. ej., bancos, compañías de seguros, corredores de títulos y valores) que es extremadamente difícil separar las dos.

Por lo tanto, para identificar y entender los requerimientos de información de una organización específica, primero es necesario entender su naturaleza y la relación inherente entre los datos y el procesamiento de información.

1.6.1.9.2 Categorías

Las organizaciones de acuerdo a la orientación de esta investigación se pueden clasificar en tres formas: (1) la organización funcional, en la que cada gerente es responsable de una área especializada, como producción, comercialización o finanzas; (2) la organización divisional, en la que cada gerente de división está a cargo de todas las funciones de dicha división; y (3) la organización matricial, en la que existen dos formas de arreglo de la organización: una en base a las funciones y otra en base a los proyectos y programas.

1.6.1.9.3 Tamaño

El tamaño de la organización es un factor que afecta los requerimientos de información. Entre más grande sea una organización, mayores serán sus

requerimientos de información. Vale la pena señalar varias características asociadas exclusivamente al tamaño.

En primer lugar, a medida que crecen las organizaciones, éstas normalmente se segmentan de acuerdo a las funciones tradicionales de las empresas.

En segundo lugar, surgen niveles gerenciales, cada uno de ellos con alcances variables de responsabilidad y autoridad. Una tercera característica asociada con el tamaño de la organización es que las comunicaciones rutinarias se vuelven más formales.

1.6.1.9.4 Estructura

La estructura de la organización es el cuarto factor inherente de la misma organización que afecta los requerimientos de información. Aun cuando la estructura está en cierta forma relacionada con el tamaño, es un factor separado debido a que dos organizaciones exactamente del mismo tamaño en términos de ventas, capital y personal, pueden diferir radicalmente en su estructura.

1.6.1.9.5 Estilo gerencial

El estilo gerencial que rige a la organización es el quinto factor organizacional que afecta a los requerimientos de información. Un estilo gerencial que incorpora conceptos de presupuestos o de costos estándar por lo general requiere más datos y procesamiento de información que aquella que considera que sólo vale la pena medir los costos reales. Un enfoque a nivel contralor requiere una información diferente a la de un en foque contable sencillo. Cualquier estilo gerencial que resalte el desarrollo de una planeación extensiva e intensiva tendrá un requerimiento correspondiente de información para pronósticos.

1.6.1.10 La información como arma competitiva

Las organizaciones operan en un mundo de desaciertos e intervención gubernamental; de políticas impredecibles a nivel monetario, fiscal, impositivo y regulador; de ciclos de negocios y recesiones; de cambios abruptos en las políticas comerciales; de competencia doméstica e internacional; de disfunciones políticas y sociales; de contracorrientes de cambio en el mercado; y de crecientes

costos laborales. A decir verdad, este es un ambiente implacable y competitivo en el que deben sobrevivir las organizaciones. Para evitar el fracaso, sobrevivir y lograr el éxito, las organizaciones deben explotar las dimensiones de la oportunidad, como se muestra en la Figura 1.5, de una gerencia informada, de la diferenciación de productos y servicios y de una creciente productividad.

La información es el arma principal que ayudará a la gerencia, a los productos y/o servicios, y a la productividad a penetrar en el ambiente competitivo. El encanto de la tecnología informática no hará avanzar estas dimensiones, pero sí lo hará la necesidad de luchar y sobrevivir en un ambiente competitivo y violento, un ambiente que incluye una competencia internacional más fuerte. Debe quedar claro que las computadoras, la tecnología informática y la información de calidad no son los fines sino simplemente las armas competitivas que apoyan a las organizaciones para alcanzar las metas de los gerentes triunfadores, de productos y servicios excelentes y de una mayor productividad y del éxito a final de cuentas. Cualquiera que sea su industria, las compañías que producen la información de la más alta calidad permanecerán como o se convertirán en las más fuertes competidoras del ramo. Por otra parte, si una compañía no puede mejorar su información, quedará a la zaga de aquellas que sí pueden.

1.6.1.10.1 Gerencia

Todas las organizaciones operan en un ambiente competitivo y a veces hostil, un ambiente que demanda ciertamente gerentes bien informados. El fracaso inminente es la alternativa para aquellas organizaciones cuyos gerentes están desinformados o mal informados. A decir verdad, el gran enemigo a vencer de la gerencia es la incertidumbre. Los gerentes deben saber qué hacer y cómo hacerlo; deben ser capaces de adaptarse a los cambios vertiginosos; deben tener acceso a la información de la organización tanto interna como externa; deben obtener señales de avisos oportunos y poder prever las amenazas y los riesgos; deben ser capaces de identificar rápidamente tanto las nuevas oportunidades como los esfuerzos inútiles.

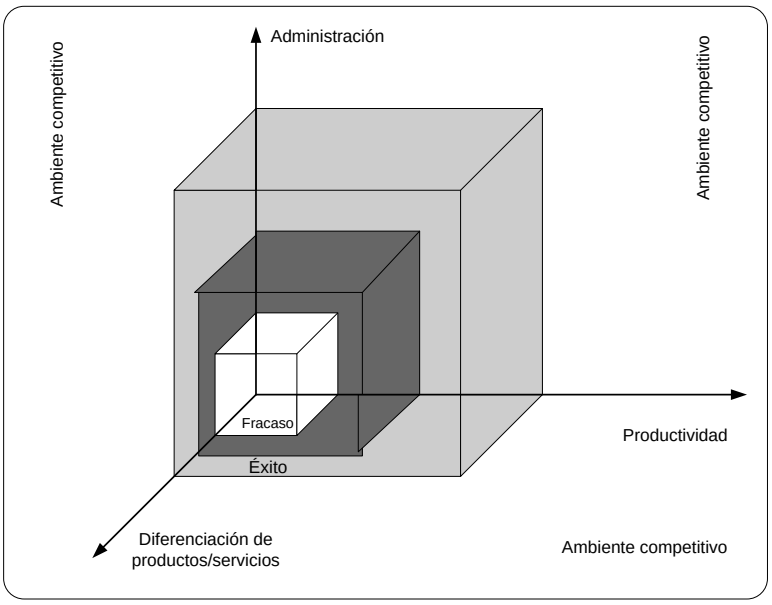


Fig. 1.5 El ambiente competitivo y las dimensiones de oportunidad de la administración, la diferenciación de productos y servicios y la productividad

La administración es, en gran medida, una función pensante. Los buenos gerentes son los iniciadores del cambio; son los líderes, los monitores, los innovadores, quienes asignan los recursos, quienes dicen adelante o alto; son los planificadores, controladores y tomadores de decisiones. La responsabilidad principal de avanzar por el espacio de las oportunidades para lograr una ventaja competitiva comienza con la gerencia. Para entender cómo ayuda la información a los gerentes a afrontar sus responsabilidades, primero se deben comprender las responsabilidades clave de la gerencia.

1.6.1.10.2 Planeación

La planeación estratégica es a largo plazo; la planeación táctica y técnica es a corto plazo. La planeación estratégica es la función principal del funcionario ejecutivo en jefe (Chief Executive Officer). La información para el soporte de la planeación estratégica sirve como el instrumento de cambio y ayuda a mover la organización del CEO en la dirección estratégica que él o ella haya elegido.

1.6.1.10.3 Control

En todas las organizaciones se requieren niveles variables de información de control.

1.6.1.10.4 Toma de decisiones

Algunos conflictos y problemas de decisión son sencillos y determinísticos y sólo tienen ramificaciones menores. Otros son complejos y probabilísticos y pueden tener un impacto significativo. La toma de decisiones puede ser rutinaria y bien estructurada, o puede ser compleja y mal estructurada. En un mundo que se concentra en los logros y las ventajas, la información puede ser el factor crítico que les permita a los gerentes y a las organizaciones obtener una ventaja competitiva.

1.7 SEGURIDAD DE LA INFORMACION[4]

La información es un recurso crítico de las organizaciones, tan fundamental como la energía o las máquinas. Es el eslabón indispensable que une a todos los componentes de la organización para una mejor operación y coordinación y para su supervivencia en un ambiente competitivo y poco amigable, las compañías actuales funcionan por la información.

1.7.1 DEFINICIÓN DE LA SEGURIDAD EN COMPUTADORAS PERSONALES

En términos simples se la puede definir como: la seguridad en computadoras personales trata de permitir que se continúe realizando el trabajo.

Una definición más académica es “libertad para disfrutar de las ventajas de las computadoras personales sin consecuencias negativas”.
Una definición más circunspecta sería “libertad para usar las computadoras sin temor a interrupciones o interferencias consideradas externas”.

1.7.2 TIPOS DE USUARIO

Las computadoras personales tienen un inmenso rango de aplicaciones, y por lo tanto un diverso rango de personas que pueden llamarse usuarios de computadoras personales. Aunque todos los usuarios responsables desean proteger sus sistemas, existe una considerable disparidad entre ellos, tanto a nivel de los ataques como del valor de los posibles daños. Las tres categorías

[4] Cobb Stephen, Manual de seguridad para PC y redes locales, 1994, Pág. 11

siguientes indican un modo de agrupar a los usuarios con respecto a sus necesidades de seguridad.

1.7.2.1 Usuarios particulares

Estas personas usan las computadoras personales para su beneficio. Los trabajos que realizan con las computadoras son para ellos, y no para una empresa. Estos usuarios son propietarios de las computadoras personales que utilizan.

1.7.2.2 Usuarios de un grupo

Son las personas que utilizan computadoras personales como parte de su trabajo para una empresa. En la mayoría de los casos, estos usuarios trabajan en computadoras propiedad de la empresa.

1.7.2.3 Usuarios responsables

Estas personas dan soporte, asistencia o gestionan grupos de usuarios. Tienen algún nivel de responsabilidad sobre los recursos de las computadoras personales de una empresa.

Obviamente, estas categorías no son rígidas o exclusivas. Se podría pertenecer sin problemas a varias, pero en cada una se tendrán que contemplar aspectos distintos de seguridad.

Desde el usuario privado preocupado por los virus en discos de juegos, al usuario de grupo preocupado por su empresa y al usuario responsable que coordina la protección de los recursos de una empresa. Los aspectos de seguridad no se aplican del mismo modo a todas las categorías por que la importancia y la responsabilidad difieren en cada una de ellas

1.7.3 ATAQUES, AMENAZAS Y TEMORES[5]

Para seguir avanzando en el tema de la seguridad en computadoras personales, es necesario utilizar un vocabulario común, además de los términos y frases

[5] Cobb Stephen, Manual de seguridad para PC y redes locales, 1994, Pág. 18

habituales de la tecnología de las microcomputadoras, se utiliza los siguientes términos:

Ataque. Término generalmente usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático personal, o intento de obtener de modo no autorizado la información confiada a una computadora personal.

Ataque activo. Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora personal o hace que se difunda de modo no autorizado información confiada a una computadora personal. Como ejemplos podemos incluir el borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ataque pasivo. Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o pinchar una red; todo esto puede dar información importante sobre el sistema, así como permitir la apropiación de los datos que contiene.

Golpe (breach). Una violación con éxito de las medidas de seguridad, como el robo de un PC o el borrado de archivos de datos valiosos.

Incidente. Cuando se produce un ataque o se materializa una amenaza, se produce un incidente; como ejemplos, están los fallos de suministro eléctrico o un intento de borrado de un archivo protegido. Es decir cualquier evento no esperado o no deseado que pueda comprometer las actividades de negocio o la seguridad de la información.

Amenaza. Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora personal. Como por ejemplo, los fallos de suministro eléctrico, virus, saboteadores o usuarios descuidados. Es decir evento que puede

desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.
Evento: Ocurrencia de un conjunto determinado de circunstancias

Las cuestiones de seguridad se han difundido gradualmente de la periferia de la comunidad de usuarios de computadoras personales hasta las salas de reuniones y juntas de responsables de todas las empresas que utilizan computadoras personales. Actualmente causan importantes inquietudes, que si se dejan sin resolver pueden descorazonar a los posibles usuarios que se beneficiarían de la potencia de las microcomputadoras Hay tres cuestiones básicas para situarse en el problema.

- ¿Qué se puede perder?
- ¿Cuáles son los orígenes de los peligros?
- ¿Cómo se puede proteger lo primero de lo segundo?
- ¿Qué puede perder?

Haciendo un mayor análisis, en 1987, la revista Government Computer News planteaba esta pregunta al Centro Nacional de Seguridad Informática (NCSC): "¿Cuáles son los principales problemas de seguridad a los que se enfrentan los responsables de los sistemas de información de las agencias gubernamentales?".

La respuesta era clara: "Uno; la falta de conciencia entre los usuarios de las computadoras, lo que trae consigo problemas de negligencia. Una de las principales razones de esta falta de conciencia es el hecho de no percibir lo que se puede perder debido a fisuras en la seguridad. Como aspecto positivo esta el que concienciar a los usuarios es más económico que instalar dispositivos adicionales de seguridad, que serán ineficaces sí los usuarios siguen siendo indolentes. Al enfatizar lo que les puede suceder a los beneficios y la productividad debido a una mala seguridad, los empleados pueden ser motivados para mostrar un mayor nivel de concienciación.

Los empleados no son los únicos responsables, si se considera el estudio de la Comisión de Auditoría del Gobierno Británico, publicado en Survey of Computer

Fraud and Mouse, realizado en más de 1.500 empresas de la muestra representativa que respondieron al cuestionario, prácticamente 180 informaron de que habían sido victimas de fraudes informáticos en los cinco años anteriores. Los fraudes iban de lo más simple a lo más complicado, e involucraban desde personal perteneciente a la cúpula de gestión hasta humildes administrativos.

En un caso típico un supervisor procesaba compras ficticias a un proveedor, enviaba el cheque al proveedor y dividía la diferencia con el supervisor. Cuando otros responsables cuestionaban las cantidades, el supervisor las atribuía a un error de la computadora y transfería las cantidades a una cuenta distinta. En otro incidente, un administrativo descubrió que los recibos descargados en un terminal remoto podían ser borrados sin que la computadora central tuviera conocimiento de ello. El administrativo borró los registros, cobró las deudas y se las embolsó.

Este estudio se realizó en 1990. Probablemente, un estudio más actualizado arrojaría un porcentaje más elevado de victimas. El estudio señalaba la difusión de computadoras personales y redes como uno de los factores principales que agravaban el problema. Debido a la existencia de dificultades inherentes a que las empresas admitan que han tenido problemas la tasa de fraude recogida estará por debajo de su valor real. Comparando los resultados frente a los obtenidos en 1987, el número de fraudes se había incrementado.

Por tanto, las computadoras personales que manejan cuentas tienden a perder dinero. Las computadoras personales manejan datos valiosos tienden a perder datos o los devalúan por una distribución no autorizada. Las computadoras personales a las que se les confía información delicada pueden causar grandes problemas si su seguridad se ve comprometida. Cuando esta información es vital para la sociedad, se puede perder muchos puntos debido a lo que la NCSC denomina “proliferación de tecnología no fiable”. Si esta o no de acuerdo con lo que el gobierno considera “intereses de la seguridad nacional”, pocas personas pueden negar que la relajación en la seguridad de las computadoras personales produzca riesgos en algo más que los simples datos.

1.7.4 ORÍGENES DEL PELIGRO

Existen muchas cuestiones que atormentan a los usuarios de computadoras personales sobre la seguridad de los datos que han confiado a una máquina que ahora resulta ser débil y accesible frente a un ataque. Por ejemplo, ¿la nueva conexión telefónica de la computadora personal incrementa la posibilidad de que nuestros archivos sean infectados por virus? ¿Cuál es la posibilidad de que la computadora personal sea atacada por un saboteador? ¿Es cierto que los datos mostrados en la pantalla de la computadora pueden ser capturados por equipos situados fuera del despacho? ¿El gobierno intenta realmente evitar que las empresas utilicen códigos secretos que él no pueda descubrir?.

Preguntas como éstas han recibido poca atención durante la loca carrera para controlar los posibles beneficios de las microcomputadoras. Aquellos que han planteado cuestiones como las anteriores han sido tachados de paranoicos, reaccionarios o dotados de una imaginación calenturienta. Actualmente, gracias a la amplia difusión de las hazañas cada vez más audaces de los “terroristas informáticos”, los usuarios normales de PC se están planteando estas cuestiones.
Informes limitados.

Desafortunadamente, las preguntas tienen mejor prensa que las respuestas. Las historias de niños prodigio que entran en redes internacionales recaban más atención que una simple lista de procedimientos administrativos que podrían haber evitado el incidente. Cuando las infecciones de virus se convierten en una noticia nacional, la gente tiende a ver virus en cada fallo o resultado erróneo de una computadora.

De hecho, el problema de los virus y los ataques de saboteadores ha ensombrecido muchos de los aspectos restantes de la seguridad informática. Es posible encontrar muchos titulares como “Otra violación de seguridad en el Departamento de Defensa” o “Los ataques de virus se recrudecen”.

A las empresas no les gusta informar de fallos de seguridad que podrían haber sido evitados fácilmente, y los temores de los usuarios de computadoras

personales son alimentados por los medios de comunicación, enturbiando el tema de las medidas preventivas. De algún modo, esta situación es natural. Hablar de intromisión, sabotaje, vandalismo, fraude y robo de computadoras implica un cierto encanto y excitación. La otra cara de la moneda es el tema poco atractivo de procedimientos reglas, seguimiento de auditoría y papeleo. De hecho, se puede incrementar en gran medida la seguridad de los datos de la computadora personal con algunos procedimientos simples de implementar.

1.7.5 AMENAZAS REALES E IMAGINARIAS.

Las posibles amenazas sobre la seguridad de los datos han sido exageradas por los medios de comunicación. La opinión pública se basa en su mayoría en noticias que informan de incidentes y robos de computadoras en un tono amenazador, reforzado con falta de exactitud y detalle. Los artículos de las revistas informáticas ofrecen un mayor detalle, pero tienen tendencia a enfatizar el lado del sensacionalismo y el impacto. De todos modos, la necesidad de proteger las computadoras personales frente a daños exteriores es cada vez mayor. Para determinar el nivel de peligro y por tanto la “respuesta adecuada”, no queda más remedio que realizar el tipo adecuado de análisis de riesgos.

A medida que se confía en las computadoras personales para realizar y compartir las tareas de gestión de información de la sociedad, sin olvidar que el diseño subyacente de estos sistemas ha evolucionado poco desde sus orígenes. Las primeras computadoras personales fueron impulsadas por un deseo de hacer llegar la informática a las masas, no para evitar que la gente accediera a información confidencial. Las computadoras personales están, por su propia naturaleza, “abiertas” a todos los usuarios. Con pocas excepciones, la computadora personal habitual de hoy en día puede ser conectada por cualquiera, utilizada por cualquiera y transportada por cualquiera.

El número de personas que saben usar una computadora personal se incrementa constantemente, así como el número de personas que pueden escribir programas para ellas. Claramente, la computadora personal está hecha para ser utilizada,

diseñada para acceder a ella libremente. Frente a esto, hay que considerar la creciente necesidad de restringir el acceso.

A la hora de determinar las posibles amenazas sobre el sistema, la mejor herramienta es una imaginación poderosa. Preguntar ¿qué podría ir mal? y ¿de qué forma podría perjudicar?. A la hora de determinar cuáles de estas amenazas son probables se necesita una fuerte dosis de realismo. Se debe hacer un análisis objetivo de la pregunta: “¿Hay alguien para quien valga la pena correr el riesgo?”. Para estimular la imaginación, considerar estas situaciones:

a) Una empresa establece un programa de “trabajo doméstico”, en el que los empleados que tienen computadoras personales en su domicilio utilizan módems para conectarse a las computadoras de la empresa, recibiendo y completando tareas a través de las líneas telefónicas. Se produce el robo del maletín de una empleada, pero a ésta le da reparo admitir que el número telefónico y la clave de acceso para conectarse a la computadora de la empresa iban en el maletín, junto con sus tarjetas de crédito. Un delincuente avezado tiene algo valioso para negociar, y un delincuente informático tiene acceso a las computadoras de la empresa. Esto puede resultar engorroso en datos estropeados, borrados o robados y vendidos al mejor postor.

b) En un descuido, un ejecutivo de BIO, 5. A., deja su maletín en el autobús urbano. Un tipo sin escrúpulos coge el maletín y la computadora portátil que contiene. Al leer el archivo de tratamiento de textos sin proteger que describe los planes para hacerse con SMALL, S. A., esta persona tiene varias opciones que van desde pedir una “recompensa” por devolver la computadora, o chantajear a BIG, 5. A., o a dar un consejo interesante a SMALL, 5. A.

c) En un descuido, un ejecutivo de BIO, S. A., deja su maletín en el autobús urbano. Un tipo sin escrúpulos coge el maletín y la computadora portátil que contiene. Al leer el archivo de hoja de cálculo sin proteger con la

contabilidad, el tipo descubre la posibilidad de chantajear al ejecutivo, que ha incluido varios pagos a una mujer que no es su esposa.

d) Las computadoras personales permiten producir documentos de gran calidad en papel oficial de las empresas. Si no se controla la distribución de los membretes, puede estar expuesto a los efectos negativos de la correspondencia no oficial. Aunque esto siempre ha resultado un problema en mayor o menor medida. la velocidad con que las computadoras personales pueden generar documentos lleva la posibilidad de abuso a un nuevo nivel.

e) Combinando programas gráficos, software de autoedición y una impresora láser, puede elaborar documentos que parezcan oficiales.

f) Utilizando recursos informáticos, muchos tipos de fraude resultan más fáciles de realizar. En un caso un responsable de ventas utilizaba cartas convincentes, pero falsas, con membretes inventados para introducir proveedores inexistentes en el libro mayor de la empresa. Entonces autorizaba recepciones inexistentes y pagos por las facturas falsas a las direcciones de los apartados postales introducidos en la cabecera.

1.7.5.1 ¿Cómo proteger del peligro lo que podría perder?

Aunque las amenazas reales son muchas y diversas, no se gana nada refugiándose en la paranoia. La seguridad se alcanza mediante una reacción equilibrada frente a las amenazas analizadas de forma realista, junto con una buena planificación de recuperación frente a desastres.

Cuando las medidas de seguridad se llevan demasiado lejos, se hacen agobiantes y pueden chocar con los beneficios primordiales del uso de computadoras personales. En situaciones en que las medidas de seguridad son inexistentes o demasiado relajadas, la dirección se verá abocada, antes o después a un crudo despertar a las realidades de los delitos informáticos y problemas causados por las computadoras en la marcha del negocio. Aunque no

se pueda prever todas las posibles amenazas contra el sistema, será posible una rápida recuperación frente a un ataque si planifica por adelantado y busca el nivel de precaución adecuado para mantener segura la información.

1.7.6 SITUACION ACTUAL DE LA SEGURIDAD[6]

Anualmente el Computer Security Institute (CSI), una prestigiosa organización formada por profesionales y empresas especializadas en seguridad informática, con la colaboración de la oficina de San Francisco Federal Bureau of Investigation's Computer Intrusión Squad, realizan la encuesta "The computer Crime and Security Survey" a los responsables de seguridad informática de organizaciones de los Estados Unidos.

A lo largo de los años, esta encuesta se ha demostrado como un fiel reflejo de las tendencias en la seguridad informática, tanto en las amenazas más importantes de cada momento, como en determinar los cambios de la percepción de la seguridad en las organizaciones.

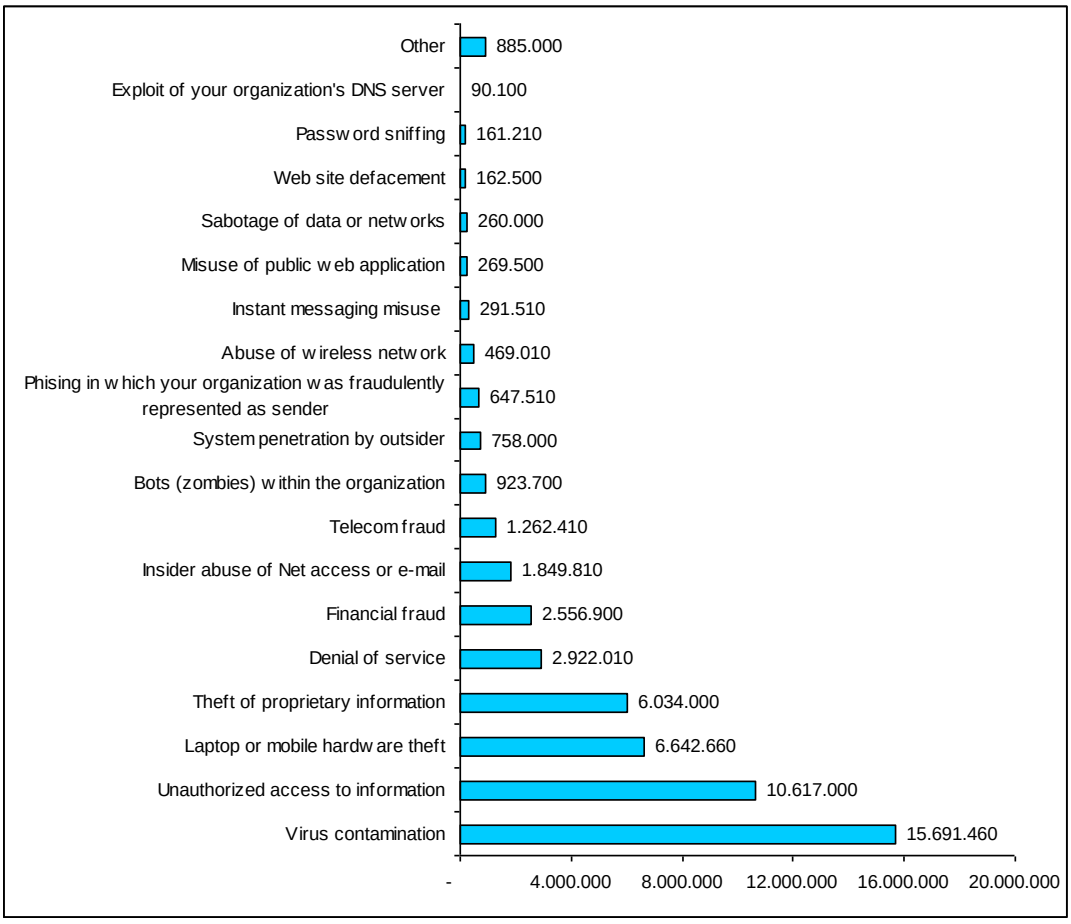
Si bien el ámbito de la encuesta se circunscribe a organizaciones de los Estados Unidos, debido al carácter global de las amenazas, prácticamente todos los datos se pueden extrapolar a organizaciones de otros países.

Este año la encuesta cumple 11 años consecutivos y fue realizada a 616 corporaciones, agencias de gobierno, instituciones financieras, organizaciones de salud y universidades que contiene aspectos como: Uso no autorizado, número de incidentes , tipo de atraques, acciones tomadas, necesidades de entrenamiento en temas de seguridad, las inversiones en temas de seguridad entre otras

Algunos de los resultados importantes del estudio de este año se resumen a continuación:

[6] CSI/FBI, Computer crime and security survey 2006, páginas 15, 16

- Los ataques del virus continúan siendo la fuente de las más grandes pérdidas financieras, el acceso desautorizado continúa siendo la segunda fuente de pérdida financiera. Las pérdidas financieras relacionaron a las computadoras portátiles (o hardware móvil) y robo de información propietaria (es decir, de la propiedad intelectual) corresponde al tercero y cuarto lugar respectivamente. Estas cuatro categorías constituyen más del 74% de pérdidas financieras, como se puede ver en la figuras 1.6 y 1.7



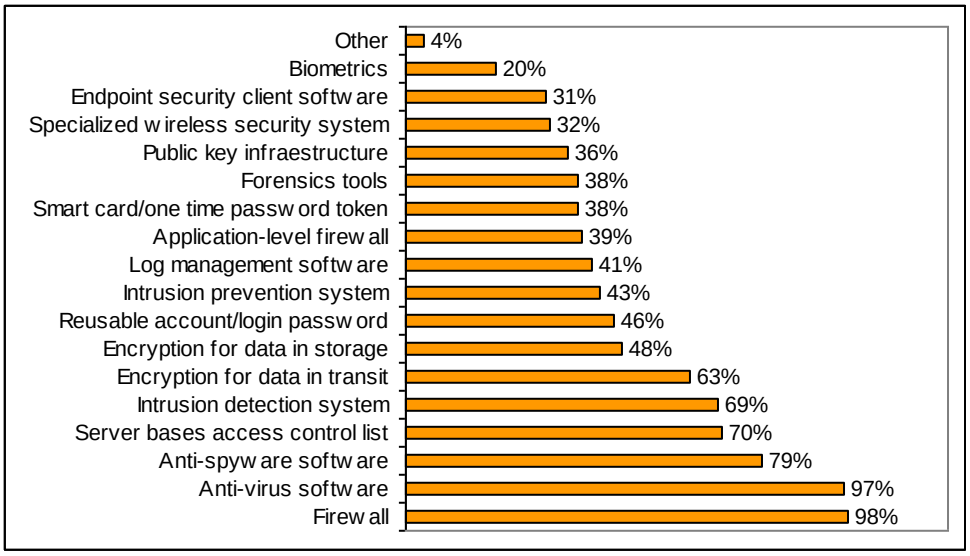
Total perdido en el 2006 = $52,494,920
Fuente: Computer Security Institute (CSI), año2006, 313 respuestas

Fig. 1.6 La cantidad dinero perdido por tipo de categoría

- El uso desautorizado de sistemas de computadora disminuyó ligeramente en este año.
- El total de dólares resultado de las pérdidas financieras han tenido un sustancial disminución este año, de acuerdo a las respuestas obtenidas. Aunque podría ser en gran parte a la disminución del número de

respuestas obtenidas así como a la capacidad de proporcionar estimaciones de las pérdidas, que también disminuyo este año substancialmente.

- A pesar de que el outsourcing se incrementa, en el estudio los resultados relacionados al outsourcing son similares al de los dos últimos años. El 61% de las organizaciones no hacen outsourcing de la función de seguridad de computadora. Entre aquéllas organizaciones que realizan outsourcing se evidencia que las actividades de seguridad, son tercerizadas en un porcentaje bastante bajo.



Fuente: Computer Security Institute (CSI), año2006, 616 respuestas

Fig. 1.7 Tecnologías de seguridad utilizada por porcentaje de respuestas

- Las organizaciones realizan la evaluación de sus inversiones de seguridad, en un 42% usando el Retorno en la Inversión (ROI), el 21% usan la Tasa Interna de Retorno (IRR), y 19% el Valor Presente (NPV). Estos porcentajes son más altos que la del último año.
- Encima de 80% de las organizaciones realizan auditorías de seguridad.
- El impacto de Sarbanes-Oxley Act, ley que impone mejores controles y auditorías para garantizar el CID de la información financiera, continúa siendo sustancial, de hecho, en los comentarios abiertos, las respuestas

demuestran complacencia en lo relacionado a la percepción de lo crítico de la seguridad que ellos enfrentan.

- Una vez más, la inmensa mayoría de las organizaciones reconocen la necesidad del conocimiento de seguridad para el personal por lo cual el entrenamiento es muy importante. Hay un aumento sustancial de hecho, en la percepción de la importancia de entrenamiento de conocimiento de seguridad. En término medio, la mayoría de encuestados no creen que la organización invierte suficiente en esta área.

1.7.7 LA EVOLUCIÓN DE LA SEGURIDAD INFORMÁTICA [7]

A lo largo de los años, la seguridad informática pasó de ser una sub-especialidad más bien oscura y exclusivamente técnica dentro del campo de la informática, para volverse una corriente de conocimientos muy extendida y con profundo impacto gerencial, que debe estar embebida en todos los aspectos de las operaciones de un área de tecnología y que debe ser incorporada al conjunto de temas y a entender y atender por parte de todo gerente de tecnología.

Adicionalmente, evolucionó de ser un conjunto de prácticas empíricas, a un cuerpo de conocimiento (Body of Knowledge - BoK) muy bien estructurado y definido, y a un conjunto de mejores prácticas altamente desarrollado y estandarizado de la industria como COBIT, ISO/IEC17799. Esta evolución no se dio de la noche a la mañana y se puede dividir en tres grandes etapas:

1.7.7.1 Las etapa de los modelos formales de seguridad

En esta etapa se formulan los primeros modelos formales de seguridad informática. Estos modelos son teóricos y usualmente están especificados en ensayos académicos en donde abundan las fórmulas de lógica de primer orden y las máquinas de estados. Tienen como objetivo mantener uno o varios de los atributos de seguridad (confidencialidad, integridad y/o disponibilidad). Son utilizados como la base teórica sobre la que se diseñan los primeros sistemas operativos, los aplicativos de autenticación, autorización y control de acceso, los sistemas de directorio, las bases de datos y los protocolos de red, entre otros.

[7] Microsoft, Actualización gerencial Mayo-Junio 2006, Páginas 16, 17 y 18

Entre los modelos más conocidos están los de Biba, HarrisonRusso-Ullman, Clark-Wilson, el de Lattice y el modelo de Chinese wall.

En esta etapa, la seguridad informática es competencia de técnicos especializados en seguridad, y se limita a esferas eminentemente técnicas, siendo considerada apenas una disciplina emergente en la academia.

1.7.7.2 La etapa de los estándares de seguridad

Se empiezan a desarrollar los cuerpos de conocimiento (Body of knowledge - BoK) de seguridad informática; organismos como ISACA e (ISC)2 empiezan a desarrollar formalmente el marco teórico de lo que más adelante se consideraría como la teoría formal de seguridad. En paralelo, organismos como la ITU, la IEEE y la ISO empiezan a desarrollar estándares de seguridad inicialmente muy técnicos y de muy bajo nivel, y, posteriormente, organismos como el NIST (National Institute of Standards and Technology), la BSI (British Standards Institute) y la ISO desarrollan estándares progresivamente más orientados a las mejores prácticas, así como a la gestión y administración de la seguridad. Se empieza a generar demanda por personas con certificados en seguridad informática como, la certificación CISM Certified Information Systems Security Professional de ISACA, y las organizaciones empiezan a incorporarlos a sus filas.

En esta etapa, la seguridad informática es de competencia directa del gerente de tecnología y se integra con la práctica de operaciones de tecnología (usualmente modelada usando ITIL), siendo tenida en cuenta para la definición de acuerdos de nivel de servicio (SLAs - Service Level Agreements) y para la planeación estratégica de tecnología.

1.7.7.2.1 Best practice - ITIL

ITIL (Information Technology Infrastructure Library), desarrollado por la CCTA (Central Computer & Telecommunication Agency), agencia del gobierno británico, tiene el objetivo de mejorar la eficacia y la calidad de los servicios informáticos y de telecomunicaciones de cualquier organismo público o privado. El objetivo de ITIL es ser un compendio de las mejores prácticas de gestión de servicios

informáticos. ITIL representa hoy la aproximación más completa y estructurada para la gestión de infraestructuras informáticas y de comunicaciones.

Por años, las organizaciones han detectado oportunidades de negocio en el uso de IT, y han hecho inversiones importantes en su infraestructura, en forma tal, que estas inversiones les permita lograr uno o varios de los siguientes objetivos:

- Reducir costos,
- Mejorar el control de gestión y el proceso de toma de decisiones,
- Ganar ventaja competitiva,
- Innovar, mejorar y rediseñar procesos,
- Facilitar procesos administrativos,
- Mejorar la calidad y funcionalidad de sus productos,
- Mejorar el servicio al cliente

Desde el punto de vista del negocio, el propósito de la gestión de la infraestructura de IT es optimizar la contribución y soporte de esta infraestructura para alcanzar sus metas de negocio. En aspectos de gestión de procesos de IT, las normas y marcos de referencia existentes dicen claramente QUE HACER, mientras que la base de conocimientos ITIL , desarrolla también en detalle el COMO HACERLO. ITIL se ha convertido en el estándar de facto en la entrega de servicios de TI para todos los tipos de organizaciones. Tanto para las organizaciones gubernamentales y no gubernamentales se benefician del manejo de los procesos a pesar del tamaño del área de TI.

1.7.7.3 La etapa de la seguridad integral

Se empiezan a ver las áreas de seguridad informática independientes del área de tecnología, en algunos momentos, incorporando elementos de seguridad industrial, seguridad física y continuidad del negocio. El presupuesto de seguridad informática se desliga del presupuesto de tecnología y se desarrollan procesos de planeación estratégica de seguridad informática y de continuidad del negocio, desligados de los procesos tradicionales de planeación estratégica de tecnología.

La gestión en seguridad informática se maneja a través de indicadores de gestión en tableros de control de gerentes a diferentes niveles jerárquicos: los riesgos informáticos hacen parte fundamental de los análisis de riesgos organizacionales, y la adquisición de infraestructura, software y servicios de seguridad informática es vista por la organización como una inversión con un retorno definido y con un propósito específico: mitigar el riesgo que afronta la misma.

Las organizaciones empiezan a buscar la forma de certificar sus operaciones de tecnología bajo estándares de seguridad reconocidos internacionalmente. Las personas con certificaciones en seguridad informática se vuelven comunes en la empresa.

En esta etapa, la seguridad informática se sale de la esfera de influencia del área de tecnología. Aparecen los CSO (Chief Security Officer), los CISC (Chief Information Security Officer) y posiciones similares en la organización, cargos de muy alto perfil jerárquico con acceso directo a la junta directiva y con poder de veto sobre proyectos de tecnología.

1.8 SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Según la Norma ISO 9000:2005. *Sistema*[8], es un conjunto de elementos mutuamente relacionados o que interactúan. Estos elementos pueden ser personas, organizaciones, secciones, sucursales, en definitiva cada una de las diversas partes que conforman un todo.

Sistema de Gestión, es un conjunto de elementos mutuamente relacionados o que interactúan para establecer la política y los objetivos y además para lograr dichos objetivos.

Sistema de Gestión de la Seguridad de la Información, entonces por las definiciones anotadas anteriormente se puede considerar que un Sistema de

[8] NTE INEN ISO 9000, año 2000, pag 8

Gestión de la Seguridad de la Información es un conjunto de procesos, procedimientos y políticas que garantizarán la confidencialidad, integridad y disponibilidad de la información de una organización.

En un concepto más amplio un Sistema de Gestión de la Seguridad de la Información (SGSI) es un sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y los planes estratégicos de la Organización.

La elección de un sistema de gestión está influenciada notablemente por las características propias de la organización, los requisitos de sus clientes a los que pretende solventar sus necesidades, los reglamentos a cumplir, así como también por las buenas prácticas internas de la empresa. Entonces, el sistema de de gestión a adoptar varía considerablemente de una empresa a otra. Sin embargo de lo anotado, en términos generales, todos los sistemas poseen prácticamente los mismos elementos a tomarse en cuenta en el momento de plantear el sistema de Gestión.

En resumen, es fácil comprobar cómo la seguridad de la información es mucho más que la seguridad informática tradicional, y es fácilmente observable como, a la hora de hablar de seguridad de la información, todo gira en torno a un eje temático: La gestión del riesgo.

Como parte de los procesos de producción las funciones de soporte están orientadas a la gestión del perímetro técnico, financiero, así como el nivel de Servicio. Estas funciones se resumen en:

Gestión de la configuración, para asegurar el control de todos los componentes de la infraestructura informática, facilitando la gestión de cambios y el tratamiento de incidencias y problemas.

Soporte a la Gestión IT, Gestión Operacional de Recursos del servicio para cumplir los objetivos de niveles de producción y calidad del servicio, mediante un proceso de coordinación que racionalice el "Workflow" de las partes y recursos implicados en la ejecución.

Control de los niveles de servicio que integra la monitorización de los indicadores y métricas del servicio (preestablecidos en los Acuerdos)

1.8.1 LA IMPLANTACIÓN DE UN SGSI

Cuando se asume la responsabilidad de gobernar las tecnologías de la información a nivel corporativo, inmediatamente se aceptan muchos retos particularmente interesantes. Estar al tanto de vulnerabilidades, parches, virus, gusanos, troyanos y ese largo etcétera de amenazas que golpean una y otra vez los sistemas de la información.

En circunstancias normales, los responsables de seguridad actúan pro activamente para prevenir los efectos perniciosos de los ataques, y cuando no hay más remedio, porque la prevención ha fallado, se actúa a posteriori. Pero, ¿se plantean los responsables antes de cualquier otra cosa de medir el riesgo que conllevan estas amenazas?

Difícil balanza la que representa colocar por un lado la cantidad de riesgo que esta dispuesto a asumir, y el otro lado la cantidad de recursos financieros disponibles para mitigar los riesgos en materia de seguridad de la información.

La gestión del riesgo se ha convertido en un escollo para la dirección estratégica de las organizaciones que confían en metodologías reconocidas para alimentar sus sistemas de gestión. Especialmente duro se hace gestionar el riesgo en aquellas empresas cuyos procesos críticos reposan en tecnologías de la información, sobre todo, cuando la seguridad de esos procesos es igualmente crítica: banca, telecomunicaciones, proveedores de acceso, proveedores de información crítica y muchas otras organizaciones donde un fallo crítico puede suponer, en el mejor de los casos, una ruptura de la continuidad del negocio. En

estos casos la gestión del riesgo deja de ser algo opcional para convertirse en algo obligatorio.

La gestión de la seguridad de la información es muy extensa, pero sin duda alguna, uno de sus puntos claves es la adecuada gestión del riesgo. Equilibrar los dos lados de la balanza, la gran mayoría de las veces, difícil de abordar, y la incertidumbre de los resultados es muy elevado, especialmente cuando no hay datos anteriores que permitan proyectar una posible tendencia. Hay riesgos incontrolables y que por tanto escapan a toda planificación. Pero esto no puede ser obstáculo para que se aparte a un lado los riesgos, y mirar al frente como si nada hubiera pasado.

Es preciso tener claro que establecer contramedidas para mitigar absolutamente todos los riesgos es algo desmesurado, por cuestiones económicas y de índole operativa, y que tampoco sería correcto asumir la totalidad de los riesgos, sin invertir en ninguna medida de control de los mismos. Es necesario llegar a un equilibrio entre inversión y riesgo asumido voluntariamente, y éste es el objetivo principal de la gestión de los riesgos.

Maneras de gestionar adecuadamente el riesgo hay muchas. Desde luego, siempre es recomendable emplear metodologías reconocidas ya que éstas emanan de una experiencia y un contraste que las hace válidas a priori.

A nivel internacional los estándares comúnmente aceptados como válidos son los que proclama la norma internacional ISO/IEC 17799:2005 A través de su metodología estructurada, busca sugerir los criterios más aceptados y las mejores prácticas de la industria para lograr una efectiva administración y gestión de la Seguridad de la Información. Con enfoque de la protección de la información de la organización y en los mecanismos utilizados para su creación, edición, transmisión y almacenamiento a través de definir:

Política de Seguridad. Es documentada, aprobada y publicada por el nivel Gerencial. Manifiesta el compromiso y enfoque de la Organización con la Seguridad.

Organización de la Seguridad de información. Establece la estructura organizativa necesaria para ejecutar, aprobar, administrar y coordinar la Seguridad Información en toda la Organización.

Administración de activos. Define un esquema para proteger los activos de la Organización a través de la asignación de responsables y controles sobre los activos.

Seguridad de recursos humanos. Busca reducir los riesgos de: error humano, robo, fraude, pérdida de confidencialidad de la información y/o uso inadecuado de las IT.

Seguridad física y ambiental. Busca impedir el acceso no autorizado, los daños, etc. sobre las instalaciones de procesamiento de información crítica o sensible.

Administración de comunicaciones y operaciones. Busca garantizar la operación de instalaciones de procesamiento de información definiendo responsabilidades y procedimientos de Operación.

Control de accesos. Establece Políticas y Procedimientos de control y administración de accesos considerando las necesidades del negocio e información.

Adquisición, desarrollo y mantenimiento de los sistemas de información. Garantizar que la seguridad es considerada e incorporada en los sistemas de información a través de controles (entrada, proceso, etc.)

Administración de incidentes de seguridad. Garantizar que los incidentes de Seguridad son identificados, clasificados, analizados / investigados, escalados y atendidos.

Continuidad del negocio. Minimizar el impacto y probabilidad de una interrupción en el procesamiento del negocio por razones de seguridad, técnicas, etc.

Cumplimiento. Verificar que el diseño, operación, uso y administración de los Sistemas de Información no infrinjan leyes, estatutos, contratos, normas, etc.

1.8.1.1 Beneficios de la implementación de un SGSI[9]

Beneficios al implantar un sistema de gestión de la seguridad de información se resumen de la siguiente manera:

- Provee a la gerencia dirección y apoyo para la seguridad en la información
- Ayuda a identificar los activos de información y a protegerlos adecuadamente
- Enfoque sistemático para el análisis y evaluación del riesgo de información en la empresa
- Reduce el riesgo del error humano, robo, fraude y el mal uso de facilidades
- Asegura una correcta y segura operación de información en la empresa.
- Incrementa sustancialmente el control de acceso a la información
- Minimiza la interrupción en el funcionamiento de las actividades del negocio y lo protege de desastres y fallas mayores (Plan de continuidad de la gestión comercial del negocio)
- Demuestra confianza al mercado, suplidores y sociedad.

1.8.1.2 Ventajas de la implantación de un SGSI

La implantación y operación de un SGSI aportará las siguientes ventajas a la organización:

- Poder disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente.

[9] www.iso27000.es/iso27000.html

- Contar con un proceso definido para Evaluar, Implementar, Mantener y Administrar la seguridad de la información.
- Diferenciarse en el marcado de otras organizaciones.
- Satisfacer requerimientos de clientes, proveedores y Organismos.
- Potenciales disminuciones de costos e inversiones.
- Formalizar las responsabilidades operativas y legales de los usuarios
- Internos y Externos de la Información.
- Cumplir con disposiciones legales (p.ej. Leyes de Protección de Datos,
- Privacidad, etc.)
- Disponer de una Metodología para poder Administrar los riesgos.

1.9 LA NORMA ISO/IEC 17799:2005 TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ISO/IEC 17799 es una guía que contiene consejos y recomendaciones (controles) que permiten garantizar la seguridad de la información en una empresa dentro de varios dominios de aplicación. Define una vía sistemática para manejar la información, que es apropiada para cualquier tipo de empresa, pero no se trata de una norma certificable.

La norma internacional ISO/IEC 17799 fue inicialmente desarrollada por el organismo British Standards Institución (BSI) como BS 7799-1. En diciembre de 2000 fue adoptada según un "procedimiento de vía rápida" por el Comité técnico mixto ISO/IEC JTC 1, Tecnologías de la Información, y publicado con las siglas ISO/IEC 17799:2000.

En Junio de 2005, la norma ISO/IEC 17799:2000 ha sido revisada de forma substancial y ha sido sustituida con efecto inmediato por la norma ISO/IEC 17799:2005. En esta nueva norma aparecen 11 dominios de controles (uno más que en la versión anterior), algunos de los dominios han sido renombrados, se

han introducido nuevos controles para gestionar una serie de temáticas no cubiertas y se han extendido otras áreas tales como la finalización de contratos o la comunicación móvil distribuida. Destaca también que en cada control se ha incluido una breve guía de implantación.

Los 11 dominios de seguridad definidos en la norma ISO/IEC 17799:2005 son los siguientes:

1) Política de seguridad: controles para proporcionar directivas y consejos de gestión para mejorar la seguridad de los datos.
2) Organización de la Seguridad de la Información: controles para facilitar la gestión de la seguridad de la información en el seno de la organización.
3) Gestión de Activos: controles para catalogar los activos y protegerlos eficazmente.
4) Seguridad de los recursos humanos: controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.
5) Seguridad física y ambiental: controles para impedir la violación, el deterioro y la perturbación de las instalaciones y datos industriales.
6) Gestión de comunicaciones y operaciones: controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.
7) Control de accesos
8) Adquisición, desarrollo y mantenimiento de los sistemas de Información: controles para garantizar que la seguridad esté incorporada a los sistemas de información.
9) Gestión de Incidentes de Seguridad de la información: controles para gestionar las incidencias que afectan a la seguridad de la Información.
10) Gestión de la continuidad del negocio: controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra averías y siniestros mayores.
11) Conformidad: controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad.

1.10 LA NORMA ISO/IEC 27001: 2005 TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - REQUERIMIENTOS

1.10.1 INTRODUCCIÓN

ISO (Organización Internacional de Estandarización) e IEC (Comisión Electrotécnica Internacional) forman un sistema especializado para la estandarización mundial. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo. En el campo de tecnología de información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC1 (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por este comité técnico son enviados a los organismos de las diferentes naciones miembros de ISO para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales en representación de su país que emiten su voto.

La norma ISO/IEC 27001 es el nuevo estándar oficial, su título completo es: BS 7799-2:2005 ISO/IEC 27001:2005 Tecnología de la información - Técnicas de seguridad - Sistema de Gestión de Seguridad de la Información – Requerimientos. Fue preparado por este JTC 1 y en el Subcomité SC 27, IT “Security Techniques”. La versión que se considerará es la primera edición, de fecha 15 de octubre de 2005, si bien en febrero de 2006 acaba de salir la versión cuatro del mismo.

El conjunto de estándares que conforman la familia ISO-2700x son:

ISO/IEC 27000	Fundamentals and vocabulary
ISO/IEC 27001	ISMS - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005

ISO/IEC 27002	Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
ISO/IEC 27003	ISMS implementation guidance (en desarrollo)
ISO/IEC 27004	Information security management measurement (en desarrollo)
ISO/IEC 27005	Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (en desarrollo)

En la norma la norma ISO/IEC 27001:2005 se presentan en detalle las etapas para el desarrollo del SGSI, para su implantación, así como aquellas para su mantenimiento. Incluye un método de evaluación, un proceso de documentación y un método de revisión que sigue el modelo Planificar-Hacer-Verificar-Actuar (PHVA) ó Plan, Do, Check, Act (PDCA).

La propuesta de la norma ISO/IEC 27001:2005, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es “Organizar la seguridad de la información”, por ello propone toda una secuencia de acciones tendientes al “establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI”. El SGSI es el punto fuerte de este estándar, los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

a. SGSI (Sistema de Gestión de la Seguridad de la Información)
b. Valoración de riegos (Risk Assesment)
c. Controles

1.10.2 DESCRIPCIÓN DE LA NORMA ISO/IEC 27001:2005

Se presenta a continuación una breve descripción de cada uno de los puntos que conforman la norma.

1.10.2.1 Generalidades

Esta norma fue preparada para proveer un modelo para establecer implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, la adopción del SGSI debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

1.10.2.2 Enfoque de procesos

Esta norma Internacional adopta un proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

Esta norma internacional adopta también el modelo "Planificar-Hacer-Verificar-Actuar (PHVA), el cual es aplicado a toda la estructura de procesos de SGSI como se muestra en la figura 1.8

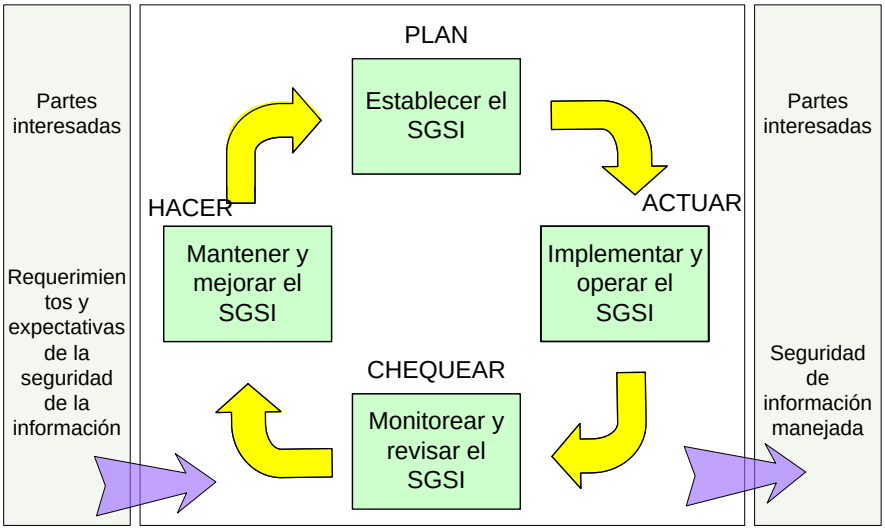


Fig. 1.8 Modelo PHVA para la Implantación de un SGSI

1.10.2.3 Compatibilidad

Se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada.

1.10.2.4 Alcance

Esta norma abarca todos los tipos de organizaciones. Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI dentro del contexto de riesgos de la organización. Especifica los requerimientos para la implementación de controles de acuerdo a las necesidades de las organizaciones o partes de ella.

1.10.2.5 Aplicación

Los requerimientos de esta norma internacional, son genéricos y aplicables a la totalidad de las organizaciones. La exclusión de los requerimientos especificados en las cláusulas 4, 5, 6, 7 y 8, no son aceptables cuando una organización solicite su conformidad con esta norma.

1.10.2.6 Referencias normativas

Para la aplicación de la norma es indispensable tener en cuenta la última versión de ISO/IEC 17799:2005, Tecnología de la información, Técnicas de seguridad, Código de práctica para la gestión de la seguridad de la información.

1.10.2.7 Términos y definiciones

Se aplican los siguientes términos y definiciones

- Activo: Cualquier cosa que tenga valor para la organización.
- Aceptación de riesgo: Decisión de aceptar un riesgo.
- Análisis de riego: Uso sistemático de la información para identificar fuentes y estimar riesgos.
- Confidencialidad: Propiedad que la información no esté disponible o pueda ser divulgada a personas, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada.

- Enunciado de aplicabilidad: Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del SGSI
- Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.
- Evaluación del riesgo: Proceso de comparar el riesgo estimado contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.
- Incidente de seguridad: uno o varios eventos de seguridad de la información, o deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.
- Sistema de Gestión de la Seguridad de la Información (SGSI): Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.
- Integridad: Propiedad de salvaguardar la exactitud e integridad de los activos
- Riesgo residual: El riesgo remanente después del tratamiento del riesgo
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
- Tratamiento del riesgo: Proceso de selección e implementación de mediciones para modificar el riesgo.
- Valoración de riesgo: Proceso general de análisis y evaluación de riesgo.

1.10.2.8 Sistema de Gestión de la Seguridad de la Información

1.10.2.8.1 Requerimientos generales

Establece lo que la organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente en un SGSI dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrenta. Para propósitos de esta norma los procesos utilizados se basan en el modelo PHVA.

1.10.2.8.2 Establecer y manejar el SGSI

Para que la organización establezca y maneje el SGSI debe:

a) Definir el alcance y límites, la política, el enfoque de la tasación del riesgo, identificar los riesgos, analizar y evaluar el riesgo, identificar y evaluar las opciones de tratamiento, seleccionar los objetivos de control y controles, obtener aprobación de los riesgos residuales, obtener la aprobación para implementar y operar el SGSI y finalmente preparar el enunciado de aplicabilidad
b) Formular un plan de tratamiento de riesgo, implementar el plan y los controles seleccionados, definir como medir la efectividad de estos últimos, capacitar, manejar las operaciones y recursos del SGSI, y finalmente implementar los procedimientos
c) Monitorear y revisar el SGSI a través de: Ejecutar los procedimientos de monitoreo, realizar revisiones, medir la efectividad de los controles, revisar las evaluaciones de riesgo, realizar auditorias, revisiones gerenciales, actualizar los planes y registrar las acciones y eventos
d) Mantener y mejorar a través de: implementar las mejoras, tomar acciones correctivas y preventivas, comunicar los resultados y acciones a todas las partes interesadas, asegurar la efectividad de las mejoras.

1.10.2.8.3 Requerimientos de documentación

La norma hace referencia que la documentación necesaria debe asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, además hay que incluir dentro de la documentación registros de las decisiones gerenciales y los resultados registrados deben reproducirse.

La documentación debe ser capaz de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y necesariamente, de regreso a la política y objetivos del SGSI.

Control de documentos.- Todos los documentos requeridos por el SGSI deben ser protegidos y controlados. Para lo cual hay que definir un procedimiento documentado que deberá establecer las acciones gerenciales necesarias para aprobar, revisar, actualizar, mantener, disponer y controlar los documentos necesarios para el SGSI.

Control de registros.- Se debe establecer y mantener registros para proporcionar evidencia de conformidad.

1.10.2.9 Responsabilidades de la gerencia

Se define como la gerencia debe proporcionar evidencias de sus compromisos para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI, además debe incluir la Gestión de recursos, Provisión de recursos y todo lo necesario para la capacitación, conocimiento, capacidad del personal.

1.10.2.10 Auditorías internas del SGSI

Existe el como la organización realizará auditorías internas al SGSI a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría.

1.10.2.11 Revisión Gerencial del SGSI

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas

revisiones incluirán valoración de oportunidades para mejorar o cambiar el ISMS incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, serán claramente documentados y deberán mantenerse registros.

1.10.2.12 Mejoramiento del SGSI

Se plantea como la organización deberá mejorar continuamente la eficiencia del SGSI a través del uso de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitoreo de eventos, las acciones preventivas y correctivas y las revisiones gerenciales. Además se define los requerimientos para la realización de las acciones correctivas y acciones preventivas.

1.10.2.13 Anexos

En esta norma también se incluye: el anexo A de esta norma propone una detallada tabla de los controles que se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 7799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en 4.2.1.

El anexo B, que es informativo, a su vez proporciona una breve guía de los principios de OECD (guía de administración de riesgos de sistemas y redes - París, (Julio del 2002, “www.oecd.org”), utilizando el modelo PDCA y los procesos descritos en las cláusulas 4, 5, 6, y 8. Por último el Anexo C, también informativo, resume la correspondencia entre esta norma y las normas ISO 9001:2000 y el ISO 14001:2004

1.10.2.14 Certificación

Desde el 15 de Octubre de 2005 las organizaciones que deseen certificar su Sistema de Gestión de la Seguridad de la Información (SGSI) pueden ser evaluadas con respecto a una nueva norma internacional ISO/IEC 27001:2005.

Esta norma sustituye a la norma británica BS 7799-2:2002, que es la que ha sido mayoritariamente utilizada hasta ese momento.

En 2814 organizaciones en 66 países han reconocido la importancia y los beneficios de esta norma, en Ecuador no existe para agosto del 2006 ningún registro de certificación, como se puede apreciar en la tabla 1.1.

Japan	1715*	Sweden	9	South Africa	2
UK	251	Spain	8	Sri Lanka	2
India	201	Turkey	7	Armenia	1
Taiwan	94	Iceland	6	Chile	1
Germany	60	Greece	5	Egypt	1
Italy	42	Philippines	5	Indonesia	1
USA	42	Kuwait	4	Lebanon	1
Korea	38	Mexico	4	Lithuania	1
Hungary	31	Saudi Arabia	4	Luxemburg	1
China	28	UAE	4	Macedonia	1
Netherlands	28	Argentina	3	Morocco	1
Singapore	24	Canada	3	New Zealand	1
Hong Kong	22	France	3	Oman	1
Australia	20	Isle of Man	3	Pakistan	1
Finland	15	Macau	3	Peru	1
Poland	15	Russian Federation	3	Qatar	1
Czech Republic	14	Slovenia	3	Romania	1
Norway	14	Bahrain	2	Serbia and Montenegro	1
Malaysia	13	Belgium	2	Thailand	1
Switzerland	13	Colombia	2	Vietnam	1
Brazil	11	Croatia	2		
Ireland	11	Denmark	2	Relative Total	2827
Austria	9	Slovak Republic	2	**Absolute Total**	**2814***

Fuente: International ISMS Register Search (Version 159 August 2006)

*The Absolute Total represents the actual number of certificates (NOTE * includes the number of ISMS certificates in Japan only available in Japanese - please refer to the JIPDEC site of the listing ONLY in Japanese). The Relative Total reflects certificates that represent multi-nation registrations or are dual-certifications. This table is copyright © ISMS International User Group 2001-2005.*

Tabla 1.1 Número de certificaciones por país

La norma ISO 27001 establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI) y complementa la norma ISO 17799, código de buenas prácticas, asegurando la selección de controles de seguridad adecuados que protejan los activos de información y ofrezcan confianza a las partes interesadas.

Una organización que obtiene la certificación es considerada que cumple la ISO 17799 y que está certificada bajo ISO 27001. Con la certificación la organización demuestra a sus socios que su sistema cumple tanto con los estándares de la norma, como también con las exigencias de controles para la seguridad, que son establecidos según sus propias necesidades.

1.10.3 DISEÑO Y PLANIFICACION DEL SGSI[10]

Siempre debe buscarse un equilibrio entre seguridad y comodidad. El fin es ayudar a la organización a sacar adelante su negocio. Si las medidas de seguridad entorpecen el trabajo de los empleados, entonces la seguridad se percibirá como un enemigo o una pesada carga con la que convivir y evitar siempre que sea posible. No tiene sentido buscar la seguridad a toda costa, sino que debe encontrarse un compromiso entre seguridad y comodidad de uso. Los usuarios deben estar informados de las razones de las medidas de se seguridad. Si entienden por qué se instauran ciertos controles, su ánimo será más cooperativo. La comodidad en función de la seguridad se representa en la figura 1.9 donde la línea de punto indica cómo a mayor seguridad, menor comodidad, y viceversa.

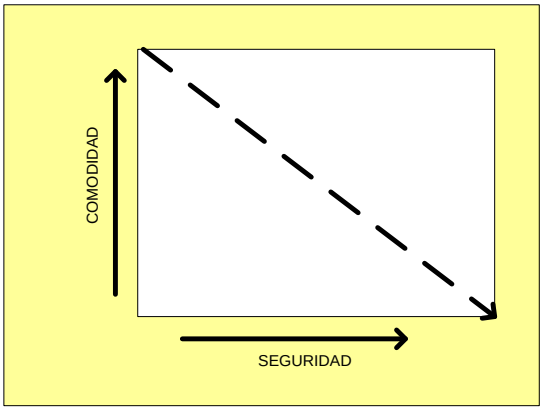


Fig. 1.9 Relación entre seguridad y comodidad

[10] ALVAREZ Gonzalo, Seguridad informática para empresas y particulares, primera edición, 2004, Pág, 12

1.10.3.1 Planificación de la seguridad[11]

Cuando se improvisa sobre la marcha, se va reaccionando a las amenazas según éstas se presentan. Un día se pierden todos los datos críticos por un fallo de hardware y a partir de entonces se pone en práctica una política de copias de respaldo, redundancia de hardware y almacenamiento distribuido para que no vuelva a pasar. Otro día un hacker entra en el servidor Web, modifica la página principal y roba la base de datos de clientes, así que a partir de entonces se instalan cortafuegos, se segmenta la red, se fortalece el servidor Web y se aísla al servidor de base de datos. De esta manera se va avanzando, a base de desastres.

Salta a la vista que una organización que solucione sus problemas mediante acciones de última hora está abocada al fracaso más que al éxito. Un componente clave para la buena marcha del negocio radica en una buena planificación, con el fin de extraer el máximo partido de los recursos disponibles. Para ello existen algunos niveles de planificación y su jerarquía que se muestran en la figura 1.10

Fig. 1.10 Pirámide de la planificación de la seguridad

1.10.3.2 Políticas de seguridad

La planificación ayuda a plantearse objetivos realistas y definir las líneas de actuación que permitan alcanzados. Una de las mejores formas de plasmar la

[11] ALVAREZ Gonzalo, Seguridad informática para empresas y particulares, primera edición, 2004, Pág, 13

actitud y expectativas de una empresa y la conducta esperada de todos sus miembros en materia de seguridad consiste en la elaboración de políticas de seguridad. Las políticas delinean las reglas que la organización espera sean seguidas por sus miembros y las consecuencias derivadas de no cumplirlas. Constituyen la piedra angular para la implantación de la seguridad. Las políticas pueden afectar a todos los recursos de la organización: hardware, software, accesos, personal, comunicaciones, redes, contratación de personal, etc., debiendo contemplar las áreas consideradas como más importantes para la organización.

Normalmente, en lugar de crearse un único documento que las cubra todas, suele subdividirse en varios documentos individuales. De esta manera, se facilita su comprensión y lectura, su distribución, su actualización cuando se realizan cambios y mejoras, así como la formación de personal en cada área. En general, el número de políticas se corresponde con el número de áreas identificadas en los objetivos de seguridad.

Una política de seguridad de la información completa y sólida suele comprender tres tipos de políticas de seguridad[12]:

- Política de seguridad de la información a nivel empresarial (Enterprise Information Security Policy o EISP): Cubre aspectos de interés para toda la empresa. Es la primera en crearse. A partir de ella se van elaborando las demás centradas en resolver problemas específicos. La política no debe experimentar cambios frecuentes, pues perdería credibilidad, debe ser firmada por la alta Dirección y estar en consonancia con la estrategia general de la organización.

- Políticas de seguridad de asuntos específicos (Issue-Specific Security Policy o ISSP): Se ocupa de asuntos específicos, como un determinado servicio de red, departamento o función, que no atañe a la organización en

[12] ALVAREZ Gonzalo, Seguridad informática para empresas y particulares, primera edición, 2004, Pág, 14

su conjunto. Normalmente constituyen una guía detallada para instruir a todo el personal en el uso de sistemas basados en la tecnología. Su propósito no es perseguir las acciones de los usuarios sino sentar las bases de lo que se considera un uso adecuado e inadecuado de la tecnología. Pueden cubrir temas como uso del correo electrónico, uso de la navegación Web, uso de fotocopiadoras e impresoras, uso del teléfono, uso de recursos de la empresa en el hogar, etc.

- Políticas de seguridad de sistemas específicos (System-Specific Policy o SysSP): Se concentran en sistemas individuales o tipos de sistemas y prescriben el hardware y software aprobados, delinean métodos para fortalecer un sistema o especifican los tipos de cortafuegos u otras medidas de control. Normalmente funcionan como estándares o procedimientos a la hora de configurar o mantener sistemas.

Desde otro punto de vista, las políticas se pueden clasificar como:

Regulatorias: discuten las regulaciones y los procedimientos a seguir cuando se aplica algún tipo de legislación o cumplimiento a la actividad de la organización;
Consultivas: que definen los comportamientos y actividades aceptables y las consecuencias de su violación, correspondiendo a esta categoría la mayor parte de las políticas; e

Informativas: que proporcionan información o conocimientos acerca de temas específicos, como objetivos de la organización o interacciones con clientes y proveedores, no siendo su cumplimiento obligatorio.

Las políticas no deben quedarse sobre el papel, sino que deben implantarse en la organización. Con tal fin, los objetivos de seguridad se formalizan, concretan y desarrollan mediante la creación de una jerarquía de documentación, de manera que cada nivel se concentra en un tipo o categoría de información y de problemas.

1.10.3.3 Estructura jerárquica de la documentación

En el nivel más alto, se encuentran las políticas de seguridad, que resumen o generalizan las necesidades de seguridad de la organización.

El siguiente nivel lo constituyen los estándares, que definen los requisitos obligatorios para el uso homogéneo de hardware, software, tecnología y controles de seguridad. En el último nivel se encuentran las normas, directrices y procedimientos

Políticas: Documentos estratégicos que especifican reglas que deben seguirse o requisitos de seguridad sobre los activos. Reciben la aprobación y apoyo de la más alta Dirección. Describen la seguridad en términos generales, sin entrar en detalles. Por ejemplo, una política de "Uso aceptable" podría cubrir las reglas y regulaciones para el uso de los recursos informáticos de la empresa y las sanciones por uso inapropiado. Para que sean efectivas, deben hacerse llegar hasta todos los miembros de la organización, quienes deben leerlas, comprenderlas y dar su conformidad. La adhesión de todos los miembros puede conseguirse por dos vías: mediante la firma del contrato laboral, que incluye entre sus cláusulas el contenido de la política o mediante la firma de un código ético o de buenas prácticas, que asimismo recoge el contenido de la política.

Estándares: Documentos tácticos que especifican el uso de la tecnología de una manera uniforme con el fin de cumplir los objetivos definidos en las políticas de seguridad. Esta estandarización de los procedimientos operativos beneficia a la organización al especificar las metodologías uniformes a utilizar en la implantación de medidas de seguridad. Los estándares normalmente son obligatorios y se implantan en toda la organización para conseguir homogeneidad.

Normas, directrices y procedimientos: Las normas definen el mínimo nivel de seguridad que cada sistema de la organización debe cumplir. Las directrices son recomendaciones que conviene seguir, pero no obligatoriamente. Son más flexibles que los estándares, ya que pueden personalizarse para cada sistema o situación únicos. Por último, los procedimientos comprenden los pasos detallados

a seguir para realizar una tarea específica. Suelen considerarse el escalón más bajo de la pirámide de las políticas. Su propósito consiste en proporcionar los pasos detallados para implantar las políticas, estándares, normas y directrices previamente creados. Las listas de comprobación (checklists) o guías de instalación y uso (how-to) son ejemplos típicos.

No se deben aglutinar los distintos niveles de documentación en un único documento, sino que cada uno debe existir como una entidad separada, organizados de forma jerárquica, como se representa en la Figura 1.11. En la cúspide de la pirámide, correspondiente a las políticas de seguridad, existirán unos pocos documentos, ya que su objetivo consiste en delinear la visión y objetivos generales de seguridad. Al descender por la pirámide, estándares, normas, directrices y procedimientos, el número de documentos crece, puesto que contienen detalles específicos correspondientes a un número limitado de sistemas, redes y áreas. Separando los documentos se facilita su mantenimiento y redistribución cuando se producen cambios y se posibilita proporcionar a cada usuario de acuerdo a sus necesidades

En muchas empresas, especialmente las de reducido tamaño, se tiene una percepción negativa de las políticas de seguridad, ya que se piensa que constituyen una pérdida de tiempo o de productividad o que sólo sirven para restringir y poner trabas al trabajo cotidiano.

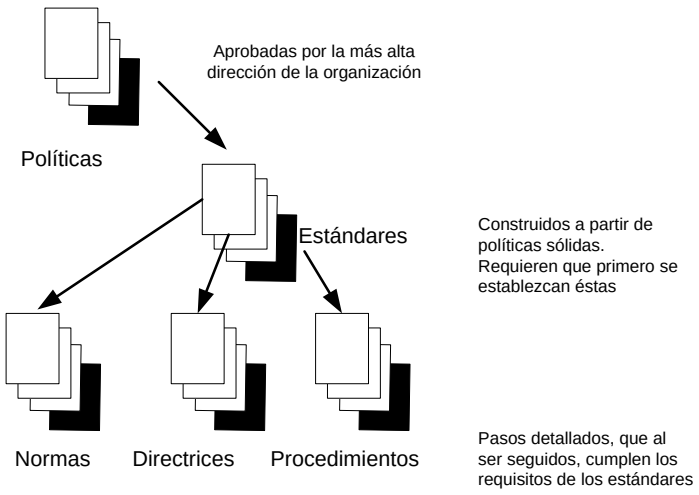


Fig. 1.11 Estructura jerárquica de la documentación

Esta visión negativa normalmente se deriva de una tensión entre las diferentes perspectivas de los miembros de una organización con respecto a los controles de seguridad:

a. A los usuarios no les gusta que les impongan reglas ni que los controlen, normalmente les importa sacar adelante su trabajo sin trabas.
b. El personal informático prefiere tener el sistema que administra bajo control, sin excesivas libertades para los usuarios, que habitualmente se traducen en más trabajo.
c. La dirección está preocupada por los costos planteados por la supuesta protección frente a las supuestas amenazas.

De estos tres grupos, normalmente los más afectados por la políticas serán los usuarios de sistemas. A los administradores las políticas también les darán más trabajo, porque en lugar de hacer las cosas a su manera o "como toda la vida", tendrán que conformarse a una serie de estándares y normas, que a veces resultan incómodos aunque como resultado final a largo plazo se obtenga una seguridad global mucho mayor. Por estos motivos, debe buscarse un equilibrio entre los requisitos impuestos a los usuarios y administradores, la pérdida de productividad y la ganancia en seguridad.

Tampoco debe pensarse que las políticas de seguridad atañen en exclusiva a las grandes organizaciones, públicas o privadas. La seguridad afecta a todos, grandes y pequeños, por lo que la planificación de la seguridad debería ser una asignatura aprobada igualmente por todos vienen a ser políticas poco elaboradas, en absoluto formalizadas, pero que reflejan cómo cada particular posee también sus expectativas y reglas en materia de seguridad. Con independencia de la dimensión de la empresa, o incluso si se trata de un particular, nunca está de más dedicar unas horas a poner por escrito estos objetivos y bosquejar unas políticas que deberán ser acatadas por todo el personal o miembros de la familia. De forma imprescindible, las políticas deben ser aplicables y hacerse cumplir, deben ser concisas y fáciles de comprender, deben equilibrar la seguridad y la productividad. Además, de forma deseable, las políticas deberían establecer las razones por las que resultan necesarias, describir los aspectos que cubren, definir funciones y responsabilidades y discutir cómo se reaccionará ante sus violaciones. Los

beneficios para la seguridad, especialmente en el caso de empresas, no tardarán en hacerse sentir.

1.10.3.4 Funciones y responsabilidades para el SGSI

No hay nada más desastroso para el funcionamiento de una empresa que no saber muy bien quién se encarga de esto, quién es responsable de aquello o a quién hay que acudir cuando ocurra tal cosa. La definición clara de funciones y responsabilidades resulta fundamental para imponer orden en este caos.

La función más importante corresponde a la Dirección, encargada de que el resto de funciones y responsabilidades se tomen en serio por los administradores y usuarios. Sin el apoyo de la Dirección, todos los esfuerzos serán inútiles. Si no se rinden cuentas de sus funciones a cada responsable, con el tiempo las conductas se relajan y los controles dejan de realizarse o no se realizan con la diligencia debida. La seguridad de la información requiere que todas las personas de la organización jueguen su parte, pequeña o grande. A menudo se tiende a percibir la seguridad como un problema tecnológico, que se resuelve a base de productos, cuando en realidad la tecnología no protege siempre y cuando no vaya soportada por personas y procesos.

1.10.3.5 Gestión del riesgo[13]

Los riesgos no pueden eliminarse por completo, en su lugar deben reducirse a niveles aceptables. La determinación de este nivel dependerá en gran medida de los objetivos concretos de la organización, del valor de sus activos, de su dimensión y presupuesto de seguridad. En primer lugar, la mayoría de problemas de seguridad reales a las que se ven expuestos los activos no tienen que ver con ataques informáticos, sino con fallos de hardware o software, errores de programación o administración, robo, fraude y extorsión, demandas legales, infracción de derechos de autor o ingeniería social, por citar algunas. En segundo lugar, los usuarios internos suponen la mayor fuente de amenazas: son los que mejor conocen el sistema, poseen acceso a veces ilimitado al mismo, saben cuáles son los activos más valiosos, en definitiva, pueden causar el daño mayor y con la mayor impunidad.

---

[13] ALVAREZ Gonzalo, Seguridad informática para empresas y particulares, Pág. 4 - 7

En consecuencia, no todas las medidas de seguridad ni las más importantes deben basarse en la tecnología y por tanto en la adquisición de software o hardware de seguridad, sino también en la organización de tareas y responsabilidades, en la gestión racional de procesos y en la formación y concienciación del personal. La seguridad de la información requiere un enfoque holístico, que implique la participación coordinada de tecnología, personas y operaciones. Su objetivo no es conseguir sistemas 100% seguros, sino sistemas tan seguros como sea necesario para proteger los activos con un nivel que se corresponda con las expectativas.

La seguridad de la información trata por tanto de proteger activos, tanto tangibles, como por ejemplo un disco duro o una base de datos con la información de clientes, como intangibles, como por ejemplo la reputación, la privacidad o el nombre de marca. Antes de implantar medidas de seguridad que no se sabe muy bien qué es lo que van a proteger ni contra qué, se debe realizar una labor previa de análisis:

- Identificar cuáles son los activos a proteger de la organización: ¿Qué activos son los más valiosos? ¿Cuál es su valor? ¿Cuánto cuesta reponerlos si se pierden o degradan? ¿Es posible reponerlos?
- Identificar las amenazas a que están expuestos los activos: ¿Cuáles son las amenazas naturales y humanas? ¿Qué agentes pueden realizar esas amenazas? ¿En qué circunstancias pueden producirse?
- Identificar los riesgos que suponen las amenazas para los activos: ¿Cuál es la probabilidad de que ocurra una amenaza? ¿Cuál es el coste tangible o intangible si la amenaza se materializa en un ataque?
- A Identificar y evaluar el coste de las contramedidas a implantar para reducir o mitigar el riesgo: ¿De qué manera puede mitigarse el riesgo? ¿Cuánto cuesta implantar una contramedida? ¿Cuál es su eficacia?

Por supuesto, este tipo de análisis no es sencillo. Debido a su complejidad, existen numerosas metodologías para la evaluación de riesgos, cada una haciendo hincapié en unos u otros aspectos. Una de las mayores dificultades prácticas de toda evaluación consiste en cuantificar el valor de los activos y el

coste asociado a los riesgos. Suelen utilizarse medidas cuantitativas, por ejemplo, la clasificación de riesgos en función de su coste económico para la organización, y medidas cualitativas, por ejemplo, la ordenación de las amenazas en función de su nivel de riesgo y en función del escenario de ataque. Otra fuente de requisitos de seguridad viene dada por el conjunto de obligaciones legales, estatutarias y regulatorias que deberá satisfacer la organización. Por último, los propios principios y objetivos de la organización impondrán sus requisitos particulares para sostener sus operaciones.

Al no existir una dirección definida ni objetivos claramente formulados, se implantan medidas de seguridad dispersas, sin documentar ni planificar, por lo que no siempre resultan adecuadas. Por lo contrario, como fruto de un análisis de riesgos, se implantarán medidas de seguridad para combatir aquellas amenazas cuyo impacto resulta crítico o que puede materializarse con mayor frecuencia, es decir, se trata de proteger los activos cuyo riesgo es mayor, según se observa en la figura 1.12.

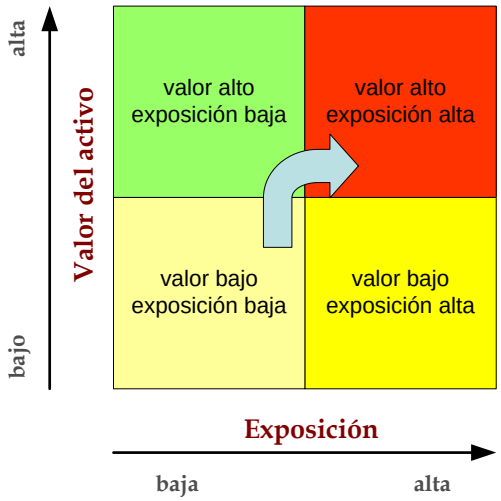


Fig. 1.12 Matriz de riesgos.

Normalmente para combatir una amenaza se intenta reducir o mitigar su riesgo mediante la implantación de salvaguardas o contramedidas. Una segunda posibilidad consiste en transferir el riesgo a otra organización, por ejemplo contratando un seguro. La tercera posibilidad consiste en asumir el riesgo, es decir, se acepta tal como es, debido a que la probabilidad de que ocurra es

demasiado pequeña o porque su coste si ocurre es inferior al de la contramedida. Al final del proceso quedará un riesgo residual, pero aceptado por la dirección.

Cuanto mayor es el valor del activo y mayor es su grado de exposición a amenazas, mayor es su riesgo y más prioritaria la exigencia de protegerlo.

El análisis, la planificación y la definición de unos objetivos de seguridad colaboran para que las medidas se implanten correctamente y no dificulten las actividades cotidianas. Como resultado, se disminuye el riesgo cumpliéndose las expectativas de seguridad. Si no se satisfacen las expectativas, habrá que revisar todo el proceso con el fin de mejorar las contramedidas, lo que puede suponer una mayor inversión, o una mejor formación y concienciación del personal, o una redefinición de los objetivos tal vez demasiado ambiciosos, o una aplicación más eficiente de la tecnología. Se sigue por tanto un proceso iterativo, hasta que las expectativas se vean siempre cumplidas, con el mínimo coste de tiempo y dinero, a la vez que se garantiza la operación normal del negocio. Después de todo, el objetivo último y prioritario de la seguridad, su verdadera razón de ser, es que la organización pueda cumplir su misión.

1.10.3.5.1 Gestión de la seguridad en el espacio

Todos los productos existentes en el mercado de seguridad informática cumplen una función de entre las siguientes:

- Prevenir: Aumentan el nivel de seguridad evitando que los ataques tengan éxito. El ejemplo clásico son los cortafuegos ó firewalls.
- Detectar: Se encargan de velar por que todo esté en orden y de alertar cuando se produce una anomalía, normalmente debida a un intruso. Un ejemplo típico es un sistema de detección de intrusos o IDS.
- Recuperar: Garantizan que ante un incidente de seguridad, causado o fortuito, se pueda recuperar toda la información y retornar a la normalidad en un tiempo mínimo. El ejemplo más conocido lo constituyen las copias de seguridad.

Estos tres pilares se realimentan unos a otros, según la relación mostrada en la Figura 1.13 la prevención evita el tener que recurrir a la recuperación, mientras que la detección facilita la recuperación y realimenta la prevención.

Para que un sistema sea razonablemente seguro, deben implantarse los tres tipos de medidas coordinadamente. Si sólo se aplican medidas preventivas, un ataque que las traspase no será detectado y será difícil recuperarse de sus daños. Si sólo se implantan medidas de detección, al no ser impedidos los ataques, continuamente estarán dando la alarma. Los efectos de aquellos ataques que pasen desapercibidos serán difíciles de mitigar. Por último, si sólo se instalan medidas de recuperación, será tal el número de ataques que causen daños, que se pasará más tiempo restaurando los datos que trabajando. Otros muchos efectos de los ataques ni siquiera se podrán subsanar.

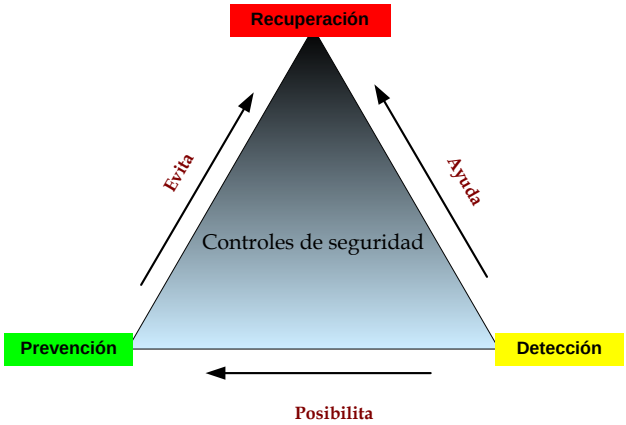


Fig. 1.13 Controles de seguridad

Para complementar estos controles de seguridad, se suelen añadir otros dos: los disuasorios y los correctivos. Estos controles pueden ser físicos, técnicos o administrativos.

- Los controles físicos incluyen el uso de candados, guardias de seguridad, tarjetas de identificación, alarmas, puertas blindadas, rejas y vallas, etc., en cuanto a la protección de locales. Por otro lado, se aplican controles similares para la protección del equipamiento informático frente a hurtos y daños por fallos eléctricos, incendios, inundaciones, etc.

- Los controles técnicos implican el uso de contramedidas incorporadas en el hardware, en el software de aplicaciones, en los dispositivos de comunicaciones, etc. Este tipo de controles recibe asimismo el nombre de controles lógicos. Comprenden los cortafuegos, antivirus, sistemas de detección de intrusos (IDS), el control de acceso, los rastros de auditoría, etc.
- Los controles administrativos comprenden el conjunto de reglas de la Dirección y procedimientos operativo s para proporcionar un grado de protección adecuado a los sistemas de información. Tienen que ver más con la administración de recursos humanos y políticas que con controles hardware y software. Entre los controles más importantes de este tipo se encuentran las políticas y procedimientos de seguridad, la formación y concienciación en seguridad del personal, la comprobación del historial del personal en los procesos de selección, la supervisión del trabajo de los empleados, la separación de funciones, los planes de recuperación de desastres y de continuidad de negocio, etc.

Evidentemente, estos controles pueden combinarse para cumplir un objetivo o utilizarse de forma independiente. De hecho, la seguridad informática debe entenderse como un proceso continuo y no como una serie de productos.

1.10.3.5.2 Gestión de la seguridad en el tiempo

La gestión de la seguridad informática debe plantearse desde una estrategia de actuación cíclica que puede subdividirse para su acometida en tres tareas principales:

- Alcanzar la seguridad: Primero se debe garantizar que la plataforma, sistemas y redes, poseen un nivel de seguridad que cumpla con las expectativas de la organización. Alcanzar este nivel de seguridad exige: fortalecer el sistema operativo, las comunicaciones de red y las aplicaciones que se ejecutan; adquirir equipos para prevenir ataques de hackers y virus; equipos que detecten estos ataques; generar rastros de auditoría para poder dar cuenta de las acciones de los usuarios legítimos e ilegítimos; instalar infraestructuras de control de acceso remoto; etc.

- Mantener la seguridad: Para garantizar que los sistemas se mantengan seguros a lo largo del tiempo habrá que desarrollar todo un grupo de políticas, normativas y procedimientos que garanticen que el trabajo del día a día no vulnera la seguridad existente. Adicionalmente, el mantenimiento y la evolución de la plataforma se realizarán de tal manera que no se vea afectada la seguridad de la organización.
- Evaluar la seguridad: Se debe realizar en paralelo una monitorización y comprobación periódica de que todos los sistemas de seguridad implicados funcionan tal y como se especifica en la política establecida y que los niveles de seguridad planteados como objetivo se corresponden con los que existen realmente. Es necesario conocer el grado real de seguridad que se posee, no el que se cree poseer. Este tipo de auditorías ayudan a identificar medidas de seguridad inexistentes, ineficaces o innecesarias.

La gestión de la seguridad se convierte por tanto en un proceso cíclico porque las amenazas, los activos y las expectativas se encuentran en continuo cambio: como resultado de la evaluación se confirmará si las medidas de control continúan siendo eficaces y adecuadas y, en caso negativo, se implantarán nuevas medidas para alcanzar un nivel de seguridad superior que habrá que mantener a lo largo del tiempo. Así se completa un nuevo ciclo de la gestión de la seguridad y vuelta a empezar.

CAPITULO 2

ANALISIS DE LA SITUACION ACTUAL DE LA EMPRESA COPCIL CONSULTORA PROFESIONAL

Basadas en la creciente competencia y complejidad de los negocios y en el permanente desarrollo tecnológico que soporta y crea nuevas oportunidades y desafíos, COPCIL se ha visto en la necesidad de contar con sistemas de información que manejen y automaticen las distintas actividades, tanto claves como de soporte, generando eficiencia y productividad, pero al mismo tiempo estructurando ambientes tecnológicos cada vez más complejos. Aspectos como: la alta sistematización de los procesos, automatización de los controles, integración de la información, y la importancia fundamental de la información para la toma de decisiones, exponen a las organizaciones a nuevos riesgos que deben ser adecuadamente administrados.

Consciente de esta situación, COPCIL, por medio de su área de Sistemas ha visto la necesidad de afrontar un proyecto de implementación de un Sistema de Gestión de la Seguridad de la Información.

Para la definición del alcance se realizó el análisis de situación actual a través de:

a. Entrevistas con los funcionarios del área de Informática y áreas usuarias destinadas a evaluar el ambiente general existente.
b. Levantamiento de la información de los procesos actuales
c. Taller para la definición del proceso crítico
d. Metodología para implantar el SGSI

2.1 LEVANTAMIENTO DE LA SITUACIÓN ACTUAL

2.1.1 INFRAESTRUCTURA TECNOLÓGICA DE COPCIL

Es necesario determinar la estructura de COPCIL en lo referente a recursos e insumos de tecnología de la información, para tener los elementos necesarios que permitan conocer la situación actual

2.1.1.1 SOFTWARE

COPCIL cuenta con el siguiente software:

2.1.1.1.1 Sistema Operativo

En las estaciones de trabajo se utiliza Windows XP y en los servidores Windows 2003 Server R2.

2.1.1.1.2 Software Utilitario

Entre los principales utilitarios utilizados podemos mencionar:

- Lotus Notes versión 6.x para correo electrónico y con base de datos de conocimiento para uso general y especializado.
- Microsoft Office XP
- Microsoft Project
- Adobe Acrobat
- WinZip
- Antivirus de MacAfee, Virus Scan Enterprise
- Microsoft Visio es una solución para crear diagramas
- Safeguard Easy de Utimaco para encriptación del disco duro.

El software detallado anteriormente se encuentra debidamente licenciado y tienen contratos de soporte y mantenimiento, lo cual permite la actualización.

2.1.1.1.3 Software de Aplicación

- El software utilizado para la gestión financiera y administrativa interna es CAPITAL, esta desarrollado en Developer 6i y utiliza la base de datos Oracle, esta solución administrativa financiera con los siguientes módulos integrados: facturación, caja-bancos, cuentas por cobrar, cuentas por pagar, activos fijos, contabilidad y presupuesto.

- La aplicación utilizada para el procesamiento de la información de recursos humanos es un ERP (Enterprise Resource Planning) de mediano rango denominado “Gestor”, sistema cuya base de datos es Oracle y su front-end está desarrollado en Developer 6i. Gestor posee los módulos de Contabilidad, Nómina, Caja/Bancos, Cuentas por Cobrar, Cuentas por

Pagar, Tesorería, Activos Fijos, Facturación e Inventarios. Este software también es utilizado para el servicio de Outsourcing de Contabilidad y Nómina que proporciona COPCIL a sus clientes.

- WIP (Work in Progress), es un software propietario que se utiliza para el control de proyectos, esta desarrollado en ASP, de Interdev de Microsoft , base datos Oracle y para los reportes Discoverer, analiza y crea informes utilizando los datos de la base de datos relacional.

- Se mantiene para consulta el software administrativo financiero utilizado anteriormente, Platinum for Windows con base de datos Pervasive SQL.

- SILEC, es un software para consultas de la legislación ecuatoriana, vigente e histórica; así como otros programas adicionales como Detform, Conesp para elaboración de reportes tributarios a organismos de control de baja complejidad.

Todos estos programas están debidamente licenciados y disponen de contratos de mantenimiento con el fabricante o su representante.

2.1.1.2 HARDWARE

Las estaciones de trabajo están conformadas por equipos notebooks IBM y un porcentaje menor de equipos desktops igualmente de marca IBM. Los equipos utilizados para servidores son servidores con procesadores Intel 70% marca IBM y el otro 30% equipos marca Compaq de la línea Proliant, como se muestra en la Tabla 2.1.

Se dispone de herramientas como Qualys para el control de seguridades en los servidores, que permite disponer de reportes de vulnerabilidades encontradas y las soluciones que permite superar las mismas. Adicionalmente el 50% de los servidores son monitoreados a través del proveedor de outsourcing, con Tivoli.

CATEGO-RIA	FABRI-CANTE	S.O.	Monitoreo contratado	USO/APLICACIÓN
GUAYAQUIL				
SERVIDOR INTEL	COMPAQ	Windows Server R2 2003	No	Software de backup,
SERVIDOR INTEL	COMPAQ	Windows Server 2000	Si	Aplicación para SW auditoría
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Almacenamiento de información
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Registro y control de usuarios
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Librería de cintas para respaldo
PC INTEL	IBM	Windows Server 2003	Si	Monitoreo e instalación
SERVIDOR INTEL	IBM	Windows Server 2003	Si	Correo electrónico y BDD de conocimiento
SERVIDOR INTEL	IBM	Windows Server 2003	No	Base de datos Oracle
PC INTEL	IBM	Windows Server 2003	No	Autenticación de acceso remoto
QUITO				
SERVIDOR INTEL	COMPAQ	Windows Server R2 2003	No	Software de backup,
SERVIDOR INTEL	COMPAQ	Windows Server 2003	No	Desarrollo- Base de datos Oracle
SERVIDOR INTEL	COMPAQ	Windows Server 2000	No	Aplicación para SW auditoría
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Registro y control de usuarios
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Almacenamiento de información
SERVIDOR INTEL	IBM	Windows Server R2 2003	Si	Librería de cintas para respaldo
PC INTEL	IBM	Windows Server 2003	Si	Monitoreo e instalación
SERVIDOR INTEL	IBM	Windows Server 2003	No	Base de datos Oracle
SERVIDOR INTEL	IBM	Windows Server 2000	No	SW Administrativo anterior para consultas
SERVIDOR INTEL	IBM	Windows Server 2000	No	WEB Server
SERVIDOR INTEL	IBM	Windows Server 2003	Si	Correo electrónico y BDD de conocimiento
SERVIDOR INTEL	IBM	Windows Server 2000	Si	SW interno para control de Riesgo
PC INTEL	IBM	Windows Server 2003	No	Autenticación de acceso remoto

Tabla 2.1 Servidores por ciudad. Elaborado por Adriana Sánchez

2.1.1.3 ESTRUCTURA ORGANIZACIONAL DEL AREA DE SISTEMAS

COPCIL cuenta con un departamento de sistemas, formado por las áreas de Administración de Redes, Administración de Bases de Datos, Soporte al usuario final y Mantenimiento de equipo electrónico, figura 2.1, cuyo principal objetivo es asesorar y asistir técnicamente en lo correspondiente al campo tecnológico informático y de comunicaciones, tiene proveedores de servicios para áreas como las de desarrollo, renta de equipos de computación, redes y comunicaciones, entre otros.

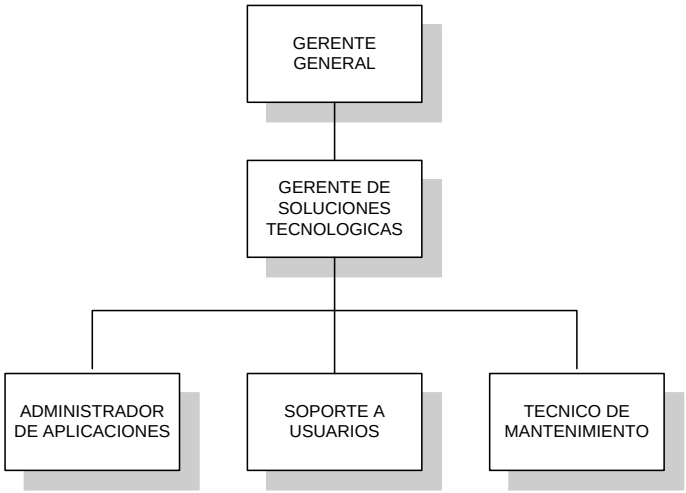


Fig. 2.1 Organigrama estructural general de la Gerencia de Soluciones Tecnológicas (GTS). Elaborado por Adriana Sánchez

El departamento de sistemas se le denomina GTS (Global Technology Solutions), brinda soporte a oficinas ubicadas en las ciudades de Quito y Guayaquil, actualmente está constituido por cuatro integrantes que coordinan todas las actividades.

En la actualidad se han firmado de contratos de outsourcing que brindan los servicios de:

- Instalación y monitoreo de servidores, provisión de hardware para estaciones de trabajo y servidores,
- Impresión y fotocopiado y
- Desarrollo de aplicaciones

Adicionalmente se cuenta con contratos de mantenimiento preventivo para los equipos electrónicos como Aire acondicionado, UPS (Uninterruptible Power Supply) y central telefónica.

2.1.1.4 REDES LAN Y WAN

COPCIL tiene dos oficinas una en la ciudad de Quito y otra en la ciudad de Guayaquil. En los dos casos son edificios de hormigón, relativamente nuevos, con instalaciones eléctricas y redes locales (LAN) adecuadas, con generadores de energía, salas de servidores con piso falso, aire acondicionado y UPS.

a. En el edificio en Quito cuenta con un UPS que abarca los equipos de computación de la sala de servidores, central telefónica y equipos activos (Switchs, hubs, routers, etc.) que es administrado para todo el edificio en forma centralizada por el arrendatario.
b. Se dispone de guardias de seguridad que controlan el acceso al edificio, y a los empleados se entrega tarjetas magnéticas para el ingreso a las oficinas, con accesos controlados de acuerdo a los requerimientos definidos.
c. Cuenta con extintores (polvo químico) en las oficinas así como en la sala de servidores.
d. En el edificio en Guayaquil se encuentran instalados varios UPS de uso exclusivo para la sala de servidores, central telefónica y equipos activos (Switchs, hubs routers, etc.) que es administrado por COPCIL.
e. El cableado estructurado es categoría 5e marca IBM y las certificaciones correspondientes de la categoría.
f. Se dispone de varios extintores en las oficinas y especialmente en la sala de servidores y áreas como la central telefónica.
g. COPCIL tiene un contrato de servicios VPN (Virtual Private Network,) para permitir el acceso remoto de los usuarios en cualquier ciudad del mundo, a costos bajos, a través de proveedores de internet.
h. Para comunicaciones remotas tipo dial-up, COPCIL tiene disponible servidores de RAS (Remote Access Service) Cisco, con líneas de comunicación dedicadas entre las oficinas de Quito y Guayaquil, la

autenticación es a través de Radius (servicio de Windows) con Username y Passwords únicos para cada persona.

Las oficinas de Quito y Guayaquil están conectadas, como se muestra en la figura 2.2, a través de un enlace dedicado punto a punto (PPP) de 512 kbps que permite la sincronización de bases de datos de Lotus Notes, transmisión de e-mails así como la conexión remota de los usuarios de Guayaquil a los servidores de bases de datos centralizados de Quito. También existe una conexión de internet de 1MB en las oficinas de Quito para conexiones internacionales de las dos oficinas

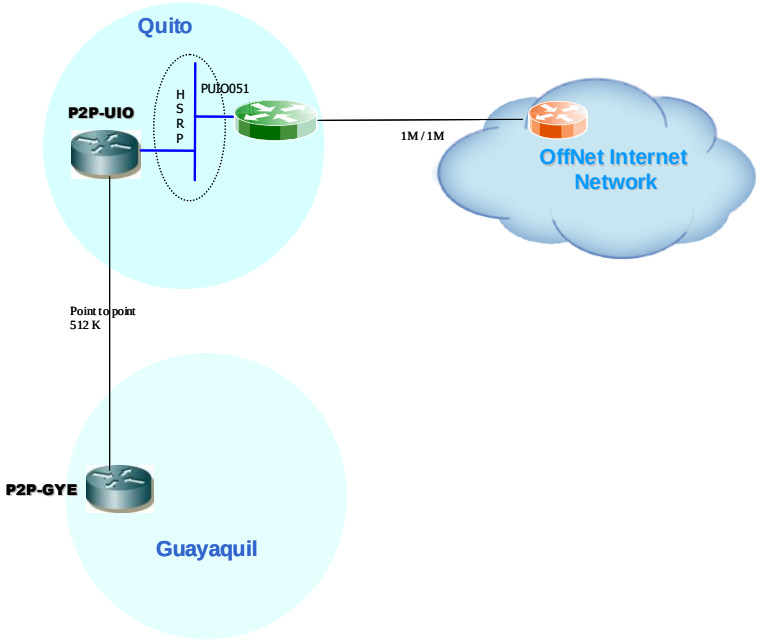


Fig. 2.2. Conexiones WAN (Wide Area Network)

2.1.1.5 TELEFONIA

Las centrales telefónicas son de marca ALCATEL para cada compañía y ciudad con extensiones conectadas a través del cableado estructurado, tabla 2.2.

Ciudad	Otras empresas	Línea externas	Centrales telefónicas	Extensiones
Quito	32	9	2	70
Guayaquil	21	8	2	45

Tabla 2.2. Telefonía disponible. Elaborado por Adriana Sánchez

2.2 DETERMINACIÓN Y DEFINICIÓN DE LOS PROCESOS ACTUALES

Como resultado del levantamiento de la información realizado en la empresa COPCIL, se ha obtenido el mapa de procesos y la representación gráfica de los subprocesos, como se puede ver en el anexo II, en el mapa de procesos se detalla los macro procesos estratégicos, de apoyo y operativos y su relación.

Esta investigación se enfoca en el macro proceso de apoyo de Gestión de Tecnologías de Información y Comunicación, en el cual se pudo determinar los siguientes procesos:

E.1 Administración de las comunicaciones
E.2 Soporte al usuario
E.3 Desarrollo de soluciones tecnológicas y
E.4 Planificación operativa

En estos procesos a su vez por su complejidad y número de actividades se determinaron los siguientes subprocesos.

N°	CODIGO	NOMBRE
1	E.1.1	Administración de red
2	E.1.2	Administración de comunicaciones
3	E.2.1	Mantenimiento de software
4	E.2.2	Mantenimiento de hardware
5	E.2.3	Mantenimiento de comunicaciones
6	E.3.1	Realizar estudio de viabilidad
7	E.3.2	Analizar requerimientos
8	E.3.3	Implantación de soluciones
9	E.4	Planificación operativa

2.2.1 DETERMINACION DEL PROCESO CRÍTICO

De acuerdo al enfoque de trabajo propuesto y acordado con COPCIL, como resultado de estos primeros análisis se determina el proceso con mayor prioridad

en la Gerencia de Soluciones Tecnológicas, de acuerdo al análisis realizado de los procesos, mediante la Matriz de Holmes, tabla 2.3.

Para la elaboración de esta matriz, se compara la prioridad entre cada uno de los procesos y se da el puntaje de acuerdo a la siguiente escala: **0** menor; **0,5** igual y **1** mayor prioridad.

Nombre del proceso	Administra-ción de las comunicaciones	Soporte al usuario	Desarrollo de soluciones tecnológicas	Planifica-ción Operativa	Total	%
Administración de las comunicaciones	0,5	0,5	1	0,5	2,5	28%
Soporte al usuario	**0,5**	**0,5**	**1**	**1**	**3**	33%
Desarrollo de soluciones tecnológicas	0	0	0,5	1	1,5	17%
Planificación operativa	0,5	0,5	0,5	0,5	2	22%
					9	100%

Tabla 2.3 Matriz de priorización de Holmes

La prioridad más alta corresponde al proceso Soporte al usuario con el 33%. Este análisis se confirma con la Matriz de enfoque ponderado, tabla 2.4, considerando cinco criterios que para COPCIL son los más representativos para su gestión. Y dando un puntaje de: **1** (mínimo) a **5** (máximo) con respecto a la contribución para alcanzar el objetivo.

Nombre del proceso	Sucepti-bilidad al cambio	Desem-peño	Impacto al usuario	Impacto en el cliente	Mejora con recursos existentes	Total	%
Administración de las comunicaciones	3	5	4	4	1	17	24%
Soporte al Usuario	**4**	**4**	**5**	**4**	**4**	**21**	**30%**
Desarrollo de soluciones tecnológicas	3	4	4	3	2	16	23%
Planificación Operativa	4	4	3	3	3	17	24%
						71	100%

Tabla 2.4 Matriz de enfoque ponderado de selección

De éste análisis se concluye que Soporte al usuario es el proceso más crítico y por tanto es el proceso que se analizará.

2.3 ESTANDARIZACIÓN DEL PROCESO CRÍTICO SELECCIONADO

Debido a la complejidad del proceso, SOPORTE AL USUARIO, éste ha sido fraccionado en tres subprocesos para facilitar su análisis y estandarización

Se deduce que al menos tres acciones básicas se podrán conseguir en área de tecnología al estandarizar este proceso:

a. Establecer un mecanismo de coordinación, de tal manera que directivos, consultores, asistentes y el personal de apoyo conozcan y cumplan los requerimientos de control de seguridad de la información, así como la política de seguridad, para que realice un adecuado uso de los equipos asignados a ellos.
b. Segundo la protección y un manejo adecuado del riesgo, para apoyar en la operación de la empresa con niveles de satisfacción interna como externa.
c. La estandarización debe apoyar el manejo de los incidentes en caso de que estos llegarán a presentarse

La estandarización por si sola no va a generar los resultados que se espera alcanzar; es el factor humano de la empresa en general, el que debe contribuir notablemente a la consecución de los resultados, y además el compromiso de alta gerencia para proporcionar los medios necesarios.
Los estándares deben convertirse en parte del pensamiento y hábitos de todos quienes hacen la organización, manteniendo continuamente un compromiso de cambio en las prácticas de trabajo para lograr los resultados esperados, en cumplimiento con la política de seguridad establecida.

En el anexo III se describe cada uno de los subprocesos, que en resumen contiene:

a. Descripción del subproceso, para cada uno de los subprocesos encontrados se han definido sus proveedores (interno, externo), insumos que ingresan, breve descripción del proceso de transformación, producto/servicio generado y finalmente los clientes (internos, externos) que hacen uso de los productos o servicios.
b. Diagrama de flujo funcional, en el cual se muestra las actividades que se realizan en el departamento de tecnología y las áreas funcionales de la empresa. Esta representación gráfica se realizó en el software Microsoft Visio 2002.

2.4 METODOLOGÍA PARA IMPLANTAR EL SGSI ISO27001:2005

Los pasos definidos en la figura 2.3, corresponde al ciclo metodológico, son los que se deben seguir para la implantación del Sistema de Gestión de la Seguridad de la Información.

Para COPCIL es importante obtener el certificado ISO 27001 esto le permitiría mostrar un valor agregado y es una herramienta del mercadeo para sus clientes, considerando sus perspectivas comerciales y de acuerdo a la tendencia en estos aspectos, considera imprescindible obtenerlo en un plazo de 3 a 4 años, para mantenerse en el mercado.

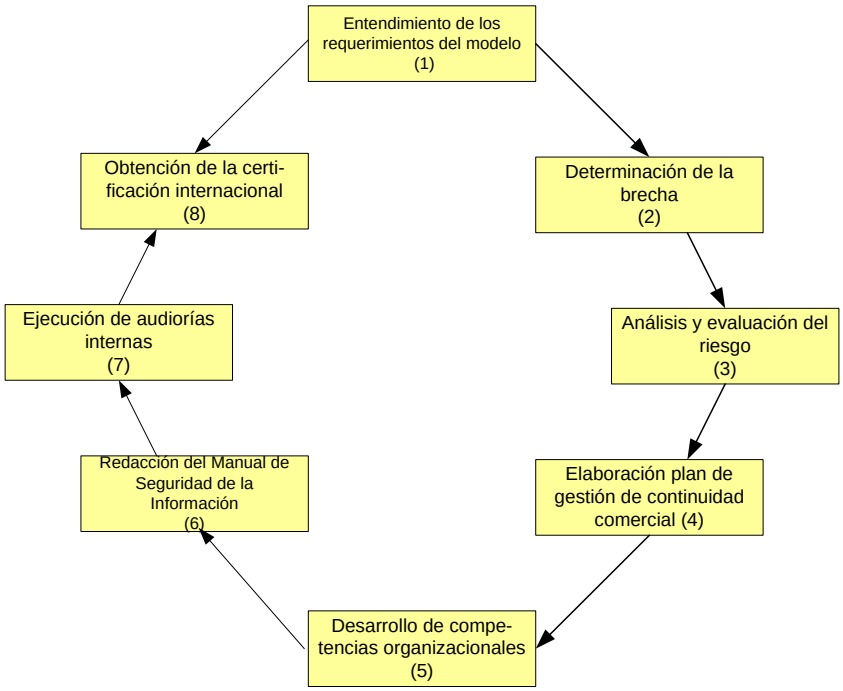


Fig. 2.3 Ciclo metodológico para la implantación del modelo ISO 27001:2005

El enfoque de este trabajo considerará los siguientes pasos:

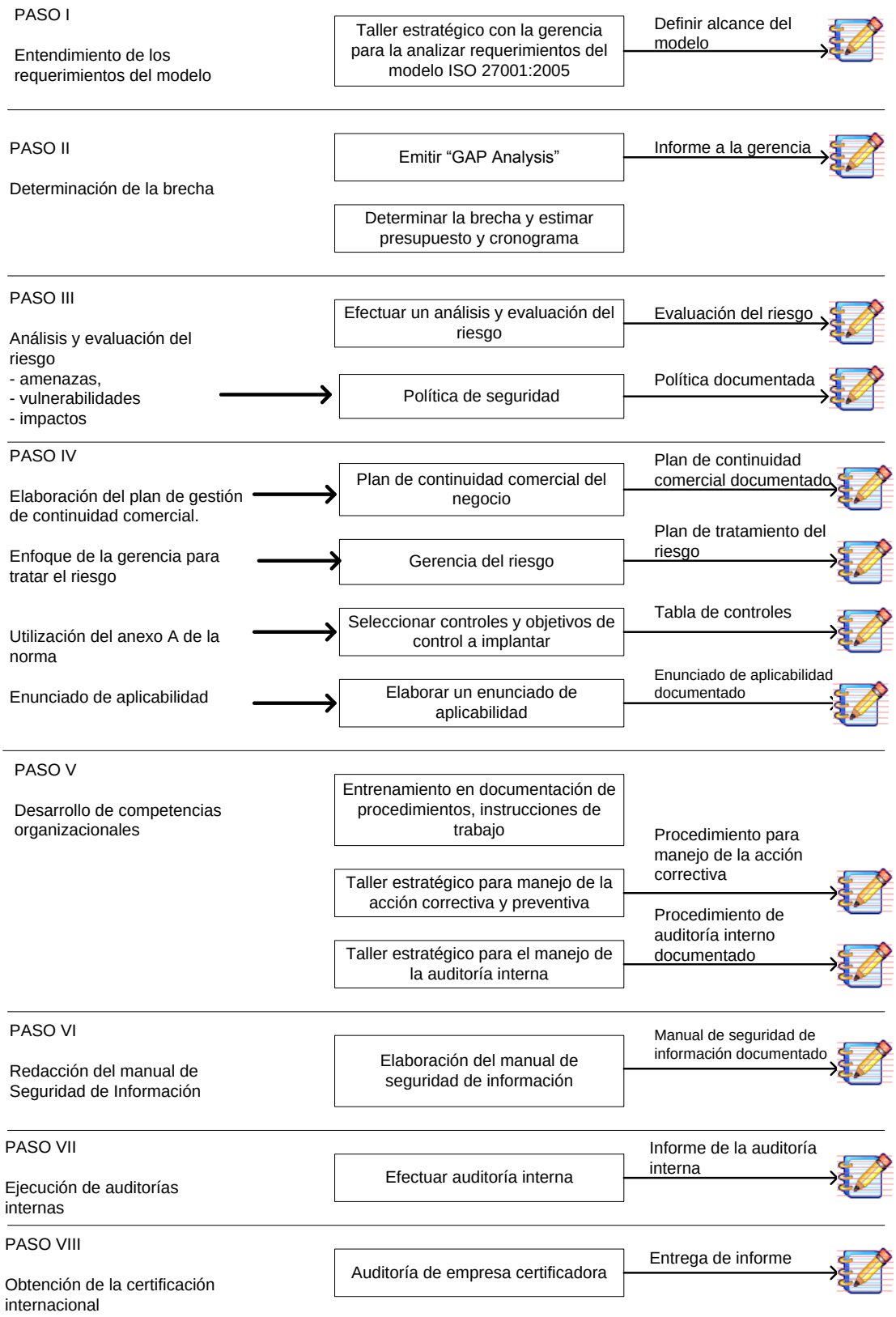


Fig. 2.4 Metodología para implementar el SGSI ISO 27001:2005 CENTRUM(Centro de Negocios Pontificia Universidad Católica del Perú)

CAPITULO 3

ANALISIS DE LA NORMA ISO/IEC 27001:2005

3.1 NATURALEZA Y DINÁMICA DE LA NORMA ISO/IEC 27001:2005, SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

3.1.1 PRINCIPIOS FUNDAMENTALES DE LA GESTIÓN DE SEGURIDAD

La norma internacional ISO 27001:2005 está orientado a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas.

Los tres principios fundamentales[14] de la gestión de la seguridad, a saber, confidencialidad, integridad y disponibilidad, denominados a menudo la tríada CID, figura 3.1, tienen relación con el objetivo de implantar los mecanismos necesarios para salvaguardar la información frente a los ataques y amenazas.

Fig. 3.1 Los principios fundamentales de la gestión de la seguridad

Confidencialidad: La información debe ser accesible únicamente a las personas autorizadas. El objetivo consiste en garantizar que los datos, objetos y recursos solamente pueden ser leídos por sus destinatarios legítimos, ya sea que están

[14] ALVAREZ GONZALO, Seguridad informática para empresas y particulares, McGrawHill, pág. 94

almacenados en algún tipo de soporte físico (disco duro, CD-ROM, etc.) o si se encuentran en tránsito entre dos equipos a través de una red de comunicaciones.
Integridad: La información debe mantenerse completa (íntegra) y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella. El objetivo consiste en garantizar que los datos, objetos y recursos no han sido alterados, permanecen completos y son fiables. La modificación no autorizada de los datos puede ocurrir durante su almacenamiento, transporte o procesamiento. Por tanto, se vuelve necesario implantar mecanismos de control de la integridad durante todos los estados de la información.

Disponibilidad: La información debe ser accesible siempre que se la necesite, durante todo el tiempo que haga falta. El objetivo consiste en garantizar que los datos permanecen accesibles sin interrupciones cuando y donde se los necesita. La disponibilidad exige que se implanten una serie de controles para asegurar un nivel razonable de rendimiento, una gestión rápida y eficiente de las interrupciones, proporcionar redundancia en caso de fallos, mantener copias de seguridad actualizadas y evitar la pérdida o destrucción de datos.

Los colaboradores en la organización asumen una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de los sistemas y tecnologías de información así como del uso de información privilegiada en la institución. Lo que refleja un compromiso personal de cada uno de ellos hacia los clientes externos e internos de la organización.

Objetivos de seguridad de información

(1) Contar con un sistema de gestión de la seguridad de información con la finalidad de mitigar los riesgos operativos y de tecnología de información.
(2) Fortalecer la cultura de administración de riesgos en función al desarrollo de valores éticos y morales respecto a la seguridad de información.
(3) Fomentar en los colaboradores la responsabilidad del manejo de la seguridad de información desde la perspectiva de la confidencialidad, integridad y disponibilidad de la información.

3.1.1.1 Modelo PDCA aplicado a los procesos SGSI

Su iniciador, el Dr. W. Edwards Deming, señalaba que la producción de bienes y servicios competitivos requieren un sistema basado en el control estadístico del proceso. El ciclo de Deming fue utilizado por los japoneses inicialmente para el desarrollo de nuevos productos, pero luego fue aplicado el ciclo en las actividades y operaciones diarias en el entorno de trabajo, el resultado fue el denominado PDCA, Figura 3.2., llamado también ciclo Deming o ciclo de control, es una de las herramientas vitales de la Calidad Total para asegurar el mejoramiento continuo.

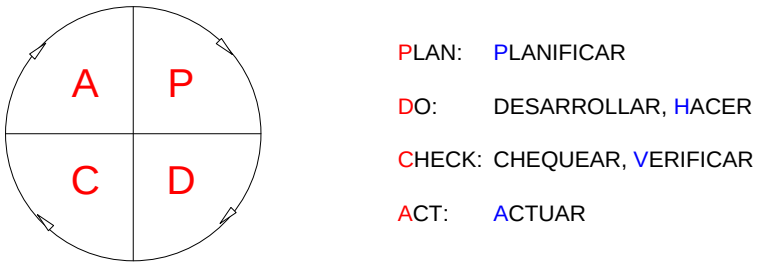


Fig. 3.2 Ciclo Deming

La norma ISO 27001:2005 adopta el modelo del proceso PDCA, el cual se puede aplicar a todos los procesos SGSI, la figura 3.3 muestra como un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. Así como muestra los vínculos en los procesos presentados en las cláusulas 4, 5, 6, 7 y 8.

Plan - Planear (Establecer el SGSI): Establecer política, objetivos, procesos, procedimientos SGSI relevantes para la administración de riesgos y mejorar la seguridad de la información para entregar resultados en concordancia a las políticas y objetivos generales de la organización.

Es decir establecer un plan para el propósito, definir las metas y los métodos que permitirán alcanzarlos, teniendo en cuenta los recursos disponibles.

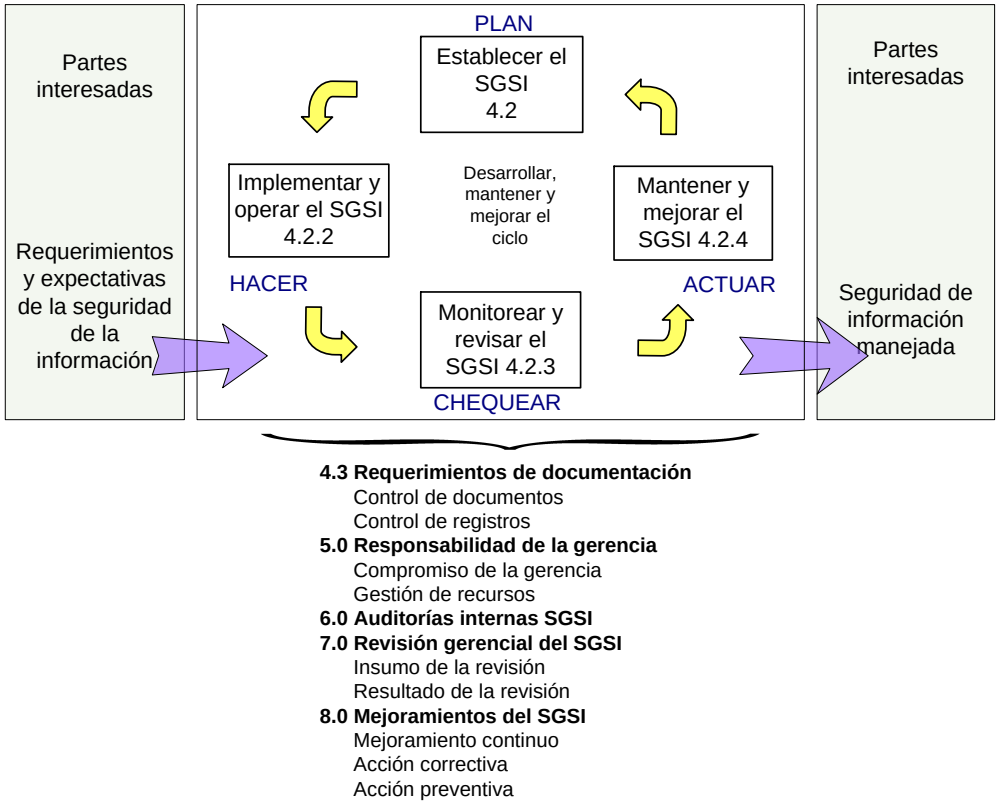


Fig. 3.3 Modelo PDCA aplicada a los procesos SGSI

Do - Hacer (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos SGSI.

Empieza esta etapa capacitando y desarrollando el personal, para que el equipo sepa por qué y cómo debe ser, realizar las tareas exactamente como fueron previstas en el plan, seguir el curso del proceso y guardar los datos para un análisis posterior

Check – Chequear (Monitorear y revisar el SGSI): Evaluar y, donde sea aplicable, medir el desempeño del proceso ejecutados en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la administración para su revisión. Es decir comparar la meta alcanzada con la planificada, es decir verificar si los resultados alcanzados concuerdan con lo planificado.

Act - Actuar (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en los resultados de las auditorías internas SGSI y la revisión gerencial o cualquier otra información relevante, para permitir la continua mejora del SGSI.

Se pretende corregir los desvíos definitivamente para que no se repitan; siempre que los resultados sean diferentes del establecido, buscar la raíz del problema; verificar si el plan fue realmente seguido; en caso afirmativo, verificar la planificación, finalmente, chequear posibles motivos de bloqueos que generalmente se encuentran en la falta de capacitación.

Esta norma internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

3.1.1.2 Estructura de la documentación requerida[15]

Un sistema de Gestión de la Seguridad de la Información basado en ISO 27001:2005 esta formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles, figura 3.4.

La documentación debe incluir los registros de las decisiones de la dirección, asegurar que se puedan seguir los indicios de las decisiones de la dirección, asegurar que se puedan seguir los indicios de las decisiones de la dirección y las políticas, así como permitir que los resultados registrados sean reproducibles.

[15] Sistema de Gestión de la seguridad de la información www.iso27000.es Pag 4

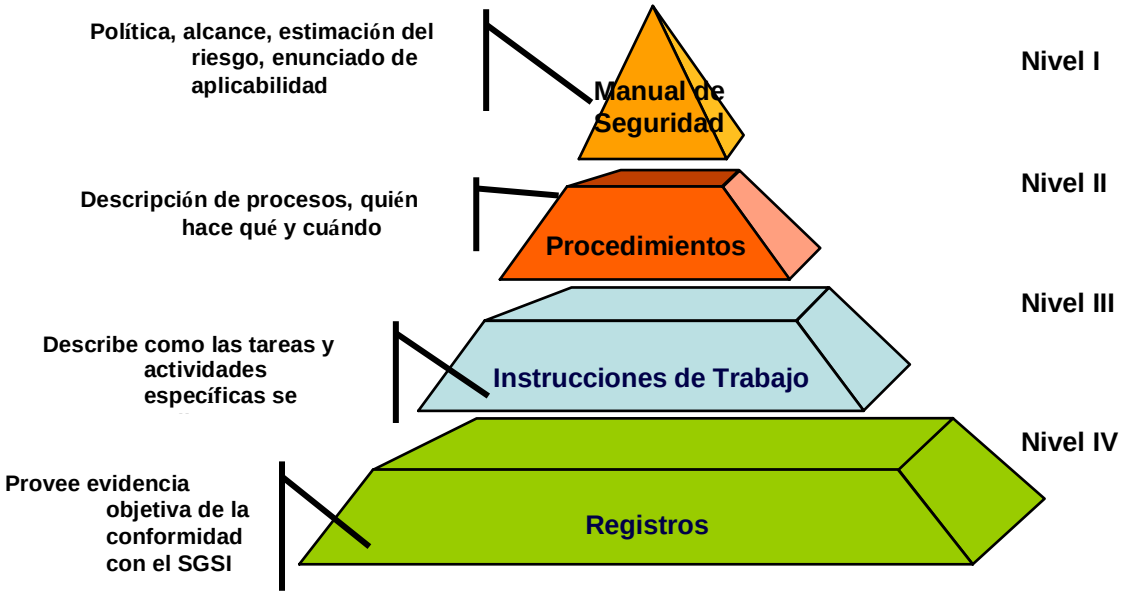


Fig. 3.4 Estructura de la documentación requerida

La documentación debe incluir:

3.1.1.2.1 Nivel I Manual de Seguridad

La administración del riesgo operacional y tecnológico en la empresa, es directamente proporcional a la gestión vía políticas y controles de sus sistemas de información. Las políticas de seguridad surgen como una herramienta organizacional para sensibilizar a los colaboradores, sobre la importancia de la información que permiten a la empresa crecer y mantenerse competitiva.

Por lo que es necesario definir una política SGSI en términos de las características del negocio, la organización, su localización activos y tecnología que:

a. Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información.
b. Tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual.
c. Establezca el contexto de la gestión organizacional y de riesgo estratégico en el cual se dará el establecimiento y mantenimiento del SGSI

d. Establezca el criterio contra el cual se evaluará el riesgo y se definirá la estructura de tasación del riesgo.

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluir una identificación clara de las dependencias, relaciones y límites que existen entre el enlace y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Metodología de evaluación de riesgos: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada.

Plan de tratamiento del riesgo: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.

Declaración de aplicabilidad (SOA Statement of Aplicability): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Procedimientos relativos al nivel 1: procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos enumerados en el nivel 1

3.1.1.2.2 Nivel II Procedimientos

El Manual de Procedimientos es el conjunto de los diferentes procedimientos que complementan al Manual de Seguridad; cada procedimiento de seguridad contiene un detalle preciso y sistematizado a través de la herramienta de la Calidad 5W + H, ¿cuándo?, ¿dónde?, ¿para qué?, ¿quién?, ¿con qué? y ¿cómo?, (When, Where, What, Who, Why y How). Su objetivo es estandarizar las actividades realizadas por el personal involucrado, garantizando la eficacia del Sistema de Gestión de la Seguridad de Información.

Procedimientos: documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

3.1.1.2.3 Nivel III Instrucciones de trabajo

Es un documento tipo que especifica qué detalles, indicaciones estructuradas, precauciones o medidas de seguridad que deben ser puestas en práctica a la hora de realizar una tarea o actividad determinada.

Es idóneo que sean redactados por el mismo personal que efectúa las tareas, y si son varias personas las que las realizan, que pongan en común sus puntos de vista, sugerencias, y conocimientos. En todo caso, debe decirse que la aplicación de una instrucción de trabajo / instrucción / procedimiento solo será eficaz si es respaldada plenamente por el Departamento en el que se realiza la actividad. Si no es así, esta perderá relevancia y habrá una marcada tendencia a ignorarla.

Instrucciones, checklist y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información

3.1.1.2.4 Nivel IV Registros

Los registros son datos que poseen significado en un medio de soporte (papel, disco magnético, óptico ó electrónico, fotografía o muestra patrón o una combinación de éstos) que presenta resultados obtenidos o proporciona

evidencia de actividades desempeñadas; los registros son los encargados de dejar constancia de los actos relativos a la seguridad de la información.

De acuerdo a la norma se deben establecer y mantener registros para proporcionar evidencia de conformidad con requerimientos y operación efectiva del SGSI, estos registros deben ser: legibles, fácilmente identificables y recuperables. Se debe implementar controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

3.1.1.2.5 Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión
- Revisar y actualizar documentos cuando sea necesario y renovar su validez
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de los documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente desechados acorde con los procedimientos aplicables según su clasificación.

- Garantizar que los documentos procedentes del exterior están identificados
- Garantizar que la distribución de documentos está controlada
- Prevenir la utilización de documentos obsoletos
- Aplicar la identificación apropiada de documentos si son retenidos por algún propósito.

3.2 ANÁLISIS E INTERPRETACIÓN DE LOS CONTROLES DE LA NORMA ISO/IEC 17799-1:2005.

3.2.1 DEFINICIONES Y GENERALIDADES

Control se define[16] como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y

En la norma ISO/IEC 17799:2005 se define a control como los medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

El control administrativo[17] es un esfuerzo sistemático para fijar niveles de desempeño con objetivos de planeación, para diseñar los sistemas de retroalimentación de la información, para comparar el desempeño real con esos niveles determinados de antemano, para determinar si hay desviaciones y medir su importancia y para tomar las medidas tendientes a garantizar que todos los recursos de la empresa se utilicen en la forma más eficaz y eficiente posible en la obtención de los objetivos organizacionales

[16] COSO [Committee of Sponsoring Organizations of the Tread way Commission. Internal Control-Integrated Framework, 1992
[17] STONER James, Administración, Pág. 657

Objetivo de control en IT se define[18] como una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de IT particular.

3.2.1.1 Enfoque para establecer requerimientos de seguridad ISO 17799:2005

Existen tres fuentes para que una organización identifique sus requerimientos de seguridad

- La primera fuente se deriva de la evaluación de los riesgos que afectan la organización. Aquí se determina las amenazas de los activos, luego se ubican las vulnerabilidades y se evalúa su posibilidad de ocurrencia y se estiman los potenciales impactos

- La segunda fuente es el aspecto legal, aquí están los requerimientos contractuales que deben cumplirse. Considerando: protección de data y privacidad de la información personal, protección de los registros organizacionales y derechos de propiedad intelectual.

- La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

Cada organización tendrá un conjunto de requerimientos diferentes de control y de niveles de confidencialidad, integridad y disponibilidad.

3.2.1.2 Controles considerados práctica común

Los controles, considerados práctica común para la seguridad de la información incluyen:

a. documento de la política de seguridad de la información;
b. asignación de responsabilidades de la seguridad de la información;
c. conocimiento, educación y capacitación en seguridad de la información;

[18] Adaptada del reporte SAC (Systems Auditability and Control Report). The Institute of Internal Auditors Research Foundation, 1991 y 1994. Pág. 163

d. procesamiento correcto en las aplicaciones;
e. gestión de la vulnerabilidad técnica;
f. gestión de la continuidad comercial;
g. gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios. Se debe considerar que aunque los controles de la norma ISO 27001:2005 son importantes, es necesario determinar la relevancia del control a la luz de los riesgos específicos que enfrenta la organización, es decir, sin perder la selección de controles basada en la evaluación del riesgo.

El nivel de seguridad alcanzado por medios técnicos demuestra ser invariablemente limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización con la dirección al frente y se debe considerar adicionalmente a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar procedimientos adecuados y la implementación de los controles de seguridad basados en la evaluación de riesgos y una medición de la eficacia de los mismos.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información, los asume, minimiza, transfiere o controla como se muestra en la figura 3.5

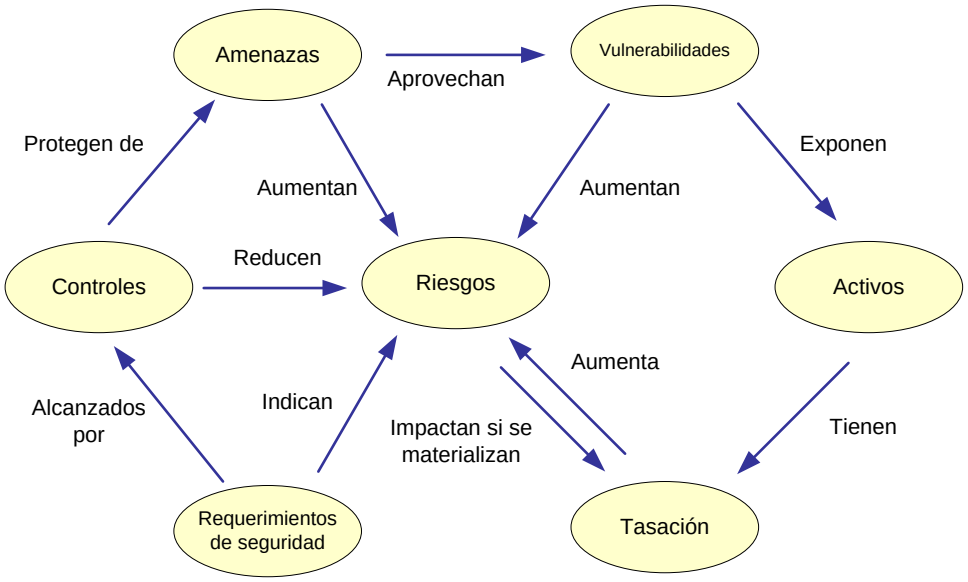


Fig. 3.5 Aspectos fundamentales del SGSI

3.2.2 ESTRUCTURA DE LA NORMA

La norma ISO 17799:2005 establece once cláusulas de control de alto nivel que cubre la gestión de seguridad como se muestra en la figura 3.6

La planificación estratégica: se realiza en los niveles directivos más altos y se ocupa de los objetivos a largo plazo de la organización, de cinco o más años. Normalmente la estrategia de de seguridad proviene de una estrategia más general que atañe a toda la organización, pero que se centra en objetivos específicos de seguridad de la información.

La planificación táctica: las frases generales de la planificación estratégica, apenas más que eslóganes, deben ir transformándose hacia objetivos concretos y aplicados. Los planes estratégicos deben utilizarse para crear planes tácticos, más centralizados en el corto plazo. Los objetivos a largo plazo de la planificación estratégica se descomponen en objetivos más inmediatos, con fechas fijadas para su consecución. La planificación táctica normalmente implica la contratación o acometida de proyectos, la adquisición de productos, elaboración de presupuestos y la elaboración de informes. El objetivo general de la dirección se traduce en objetivos más concretos.

Fig. 3.6 Estructura de seguridad de la información

La planificación operativa: los planes operativos se derivan de los planes tácticos con el fin de organizar las tareas del día a día, es decir se va dando forma concreta a los objetivos tácticos. De estos se derivan un total de 39 objetivos de control que son resultados que se esperan alcanzar mediante la implementación de controles, estos son prácticas, procedimientos o mecanismos que reducen el nivel de riesgo, la norma tiene 133 controles específicos como se muestra en tabla 3.1,

Cada categoría de seguridad contiene:

a. Un objetivo de control que establece lo que se debería lograr; y
b. Uno o más controles que se puedan aplicar para lograr el objetivo.

ISO 27001:2005		Categoría de control	Controles
A.5	Política de seguridad	1	2
A.6	Organización de la seguridad de la información	2	11
A.7	Gestión de archivos	2	5
A.8	Seguridad de los recursos humanos	3	9
A.9	Seguridad física y ambiental	2	13
A.10	Gestión de las comunicaciones y operaciones	10	32
A.11	Control de acceso	7	25
A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información	6	16
A.13	Gestión de incidentes en la seguridad de la información	2	5
A.14	Gestión de la continuidad comercial	1	5
A.15	Cumplimiento	3	10
Total	**11**	**39**	**133**

Tabla 3.1 Estructura de la ISO 27001:2005

3.2.3 CRITERIOS DE IMPLANTACIÓN DE UN SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)[19]

Para establecer y gestionar un SGSI en base a ISO 27001:2005, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad, esto se muestra en la figura 3.7

: Plan (planificar): establecer el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorizar y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI.

3.2.3.1 PLAN. Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:

[19] www.iso27000.es

  - Incluya el marco general y los objetivos de seguridad de la información de la organización;
  - Considere requerimientos legales o contractuales relativos a la seguridad de la información;
  - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
  - Establezca los criterios con los que se va a evaluar el riesgo;
  - Esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los riesgos. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y reproducibles. (Existen distintas metodologías para la evaluación de riesgos y se pueden encontrar algunos ejemplos en la guía para la gestión de la seguridad ISO 13335-3.)
- Identificar los riesgos:
  - Identificar los activos que están dentro del alcance del SGSI ya sus responsables directos, denominados propietarios;
  - Identificar las amenazas en relación a los activos;
  - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
  - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos:
  - Evaluar el impacto en el negocio de la organización de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
  - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
  - Estimar los niveles de riesgo;
  - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
    - Aplicar controles adecuados;
    - Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y Criterios establecidos para la aceptación de los riesgos;
    - Evitar el riesgo, por ej. mediante el cese de las actividades que lo originan;
    - Transferir el riesgosa terceros, por ej. aseguradoras o proveedores.
- Seleccionar los objetivos de control y los controles del Anexo A de la norma ISO 27001 para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
    - Los objetivos de control y controles seleccionados y los motivos para su elección;
    - Los objetivos de control y controles que actualmente ya están implantados;
    - Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión. Este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.
- En relación a los controles de seguridad, el estándar ISO/IEC 17799 proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 cláusulas.
- El estándar ISO 27001 referencia en su segunda cláusula a la guía ISO/IEC 17799 en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso que la guía no contemplase ciertas necesidades particulares.

Fig. 3.7 Implementación del SGSI

3.2.3.2 DO. Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados y que incluya la financiación, la asignación de roles y responsabilidades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados.
- Procurar programas de formación y concienciación en relación a la seguridad de la información dirigidos a todo el personal.
- Gestionar las operaciones del SGSI.

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

3.2.3.3 CHECK. Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
    - La detección temprana de errores en los resultados generados por los procesos;
    - La identificación temprana de brechas e incidentes de seguridad;
    - Capacitar a la dirección para determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
    - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo. los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

3.2.3.4 ACT: Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la Cláusula 8 de la norma ISO 27001 ya las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

Uno de los componentes primordiales en la implantación exitosa de un sistema de gestión de la seguridad de la información es la implicación de la dirección. Debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos.

3.2.3.5 Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

3.2.3.6 Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.

- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

3.2.3.7 Formación y concienciación

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado y se

- Determinen las competencias necesarias para el personal que realiza tareas en aplicación del SGSI,
- Satisfagan dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado,
- Evalúe la eficacia de las acciones realizadas,
- Mantengan registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante está concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

3.2.3.8 Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.

- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de efectividad.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requerimientos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

3.2.3.9 Factores críticos del éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a. Política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales;
b. Un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;

c. Soporte visible y compromiso de todos los niveles de gestión;
d. Un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;
e. Marketing efectivo de la seguridad de la información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema;
f. Distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas;
g. Provisión para el financiamiento de las actividades de gestión de la seguridad de la información;
h. Proveer el conocimiento, capacitación y educación apropiados;
i. Establecer un proceso de gestión de incidentes de seguridad de la información;
j. Implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

CAPITULO 4

DESARROLLO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

4.1 ESTRUCTURA DE LA DOCUMENTACION BASICA DEL SGSI

4.1.1 INTRODUCCION

La seguridad constituye el equilibrio entre la capacidad para mantener la facilidad de uso de los recursos en la organización y, a su vez, controlar el acceso a dichos recursos, COPCIL Consultora Profesional es una empresa de servicios, que basa su negocio en la información, que junto a los procesos, a las personas y a los sistemas que hacen uso de ella, constituyen los activos más importantes para la empresa, los mismos que enfrenta amenazas que podrían explotar las vulnerabilidades existentes, que a su vez, podrían dañar de alguna forma los activos de la organización, por tanto es necesario analizar estos riesgos de seguridad potenciales para minimizar, transferir o controlar el impacto y las consecuencias.

La confidencialidad, integridad y disponibilidad de la información en la empresa, es fundamental para el aumento de la competitividad, rentabilidad, conformidad legal e imagen de la empresa, por tanto requiere:

a. Identificar las aplicaciones que procesan y guardan la información, y el valor que esta información tiene para la empresa.
b. Conocer el impacto de la divulgación o la falta de disponibilidad de estos activos de información para el negocio.
c. Determinar los controles actuales y los necesarios para proteger estos activos y finalmente
d. La identificación y elaboración de los procedimientos para la implementación, así como la administración responsable del riesgo.

Puntos básicos que le permitirán la elaboración de un Sistema de Gestión de la Seguridad de la Información, que Copcil, considera como un valor agregado y una herramienta del mercadeo para lograr sus objetivos de negocio.

De acuerdo al análisis del proceso crítico realizado en el capítulo 2 literal 2.2.1, se definió la realización del SGSI para el proceso “Soporte al usuario” de la Gerencia de Tecnologías de la Información.

Un Sistema de Gestión de la Seguridad de la Información basada en ISO/IEC 27001:2005 está formado por una serie de documentos, como se muestra en la figura 3.4 del capitulo 3, que se la puede clasificar en:

- Manual de seguridad
- Procedimientos
- Instrucciones de trabajo
- Registros

4.1.2 MANUAL DE SEGURIDAD

De acuerdo a la cláusula 4.2.1 de la norma ISO/IEC 27001:2005 para establecer el SGSI es necesario:

a. Definir el alcance y los límites del SGSI en términos de las características del negocio.
b. Definir una política del SGSI
c. Definir el enfoque de tasación del riesgo de la organización
d. Identificar los riesgos
e. Analizar y evaluar el riesgo
f. Identificar y evaluar las opciones para el tratamiento de los riesgos
g. Seleccionar objetivos de control y controles para el tratamiento de riesgo
h. Obtener la aprobación de la gerencia para los riesgos residuales, así como su aprobación para implementar y operar el SGSI.
i. Obtener la autorización de la gerencia para implementar y operar el SGSI
j. Finalmente preparar el enunciado de aplicabilidad

El desarrollo de los puntos descritos anteriormente se encuentran en el ANEXO IX a excepción de los literales g y h que no son parte de los objetivos de este trabajo.

4.1.3 DETERMINACIÓN DE LOS ACTIVOS DE INFORMACIÓN[20]

Para identificar los activos se utilizo el método de la elipse concéntrica, que permite identificar los distintos tipos de activos de información existentes dentro del proceso soporte al usuario del área de Tecnologías de Información, como se muestra en la figura 4.1.

Este método comprende:

a. En la elipse interna se puede visualizar los subprocesos que componen el proceso de Soporte al usuario que son: *requerimiento de servicio*, mantenimiento de software, hardware y comunicaciones.
b. En la elipse intermedia se identifican los dueños de estos procesos, los activos de información vitales y las interacciones representadas por las flechas.
c. En la elipse externa se identifican las organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse, aquí también debe identificarse los activos de información, con miras a averiguar el tipo de convenio que existe o debería de elaborarse, así como los contratos existentes y los grados de acuerdos necesarios.

[20] CLAPAM Comisión Latinoamericana de Productividad y Medio Ambiente

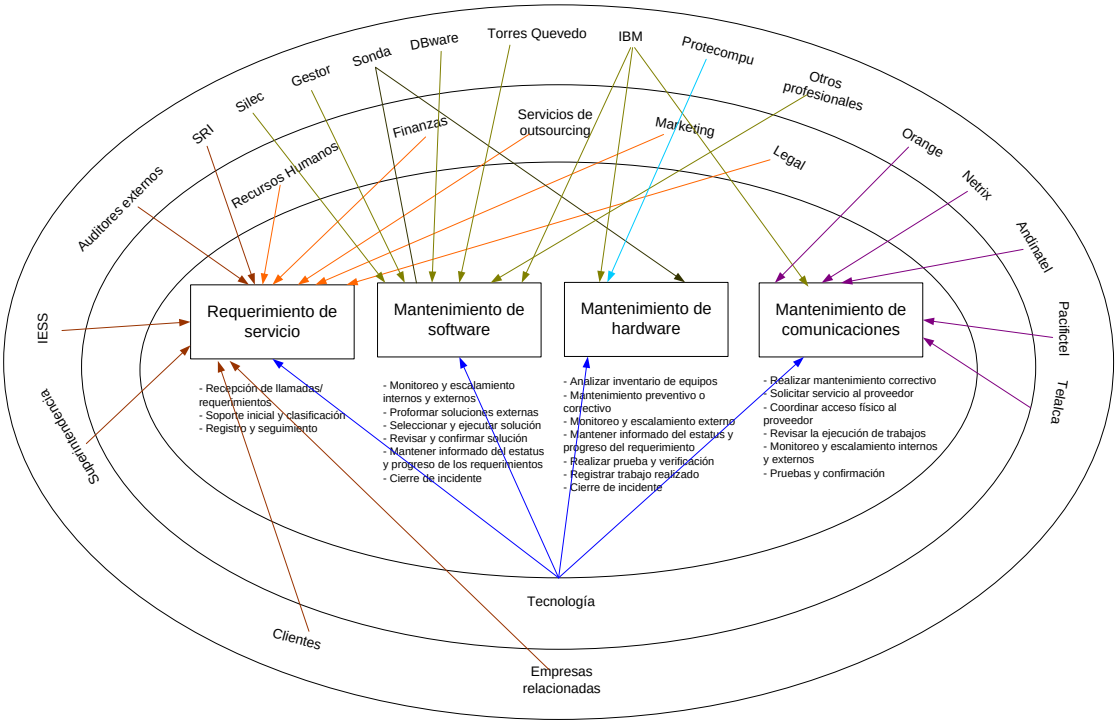


Fig. 4.1. Elipse concéntrica del proceso E.1.1. Soporte al usuario
Elaborado por Adriana Sánchez

4.2 ANÁLISIS Y EVALUACIÓN DEL RIESGO

De acuerdo a la sección 4.2.1 de la norma ISO 27001:2005 se efectúa el análisis y evaluación del riesgo de los activos identificados, siguiendo los pasos metodológicos que se muestran en la figura 4.2, de una manera disciplinada y sistemática.

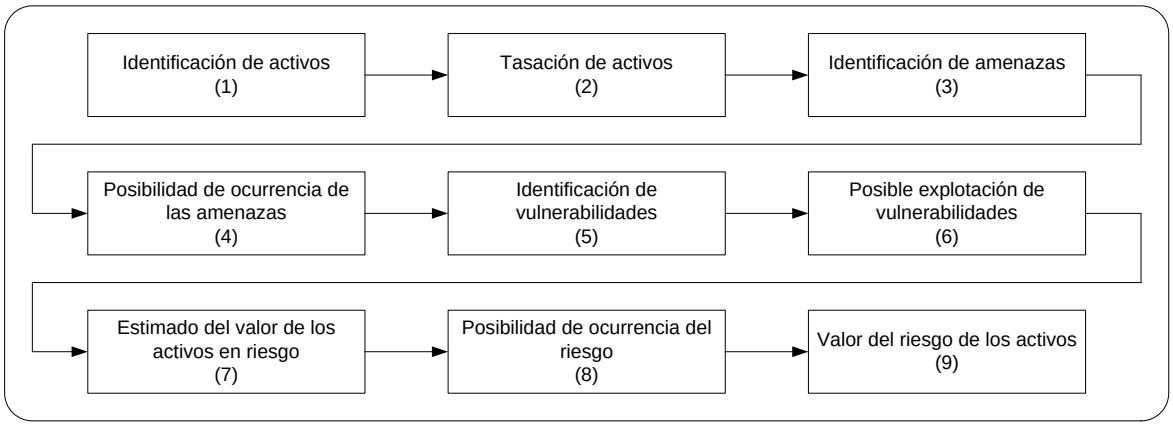


Fig. 4.2 Metodología para el análisis y evaluación del riesgo Fuente: CAPLAM

Paso (1) Identificación de activos.

En el anexo IV se muestra la lista de 48 activos de información involucrados en el proceso “Soporte al usuario” de la empresa Copcil, que es el resultado del uso de la metodología de elipses concéntricas.

Paso (2) Tasación de activos.

Para identificar la protección apropiada a los activos; es necesario tasar su valor en términos de la importancia para la organización; la valoración del activo se realiza en forma cualitativa así como del valor de la información que contiene cada uno de esos activos y de la forma que se relacionan con otros activos en su entorno, para poder planear adecuadamente las contramedidas y protecciones que mitiguen el impacto se tasa en relación a la confidencialidad, integridad y disponibilidad, mediante una escala del 1 al 5, donde:

muy bajo	**bajo**	**medio**	**alto**	**muy alto**
1	2	3	4	5

Los resultados obtenidos de la tasación del riesgo se muestran en el anexo V, que en síntesis establece lo siguiente:

Número de activos	Puntaje
28	5
11	4
8	3
1	2

A partir de este paso se realizará la evaluación para los activos con mayor puntaje (5) que representan los activos que producirían el mayor impacto en las operaciones de Copcil:

1. Centrales telefónicas
2. Datos del cliente
3. Desktop (Hw y Sw)
4. DTU
5. Firewall
6. Informes y reportes impresos o electrónicos
7. Librerías de respaldo
8. Líneas telefónicas
9. Multifuncionales
10. Notebooks (Hw y Sw)
11. Personal interno que da soporte
12. Personal de la empresa de outsourcing que brinda servicios
13. Routers
14. Servicios de comunicaciones de proveedores
15. Servicios de IT de proveedores
16. Servidor de almacenamiento (storage)
17. Servidor de aplicaciones de riesgo
18. Servidor de aplicaciones WEB
19. Servidor de archivos
20. Servidor de base de datos Oracle
21. Servidor de correo electrónico y BDD de LN

22. Servidor de Radius (acceso remoto)
23. Sistema de discos
24. Software Contable Financiero CAPITAL
25. Software Contable para servicio de Outsourcing GESTOR
26. Software Control de proyectos WIP
27. Software para Encuesta salarial SIREM
28. Switchs

Paso (3) Identificación de Amenazas.

A través de una dinámica de grupos utilizando la técnica de "lluvia de ideas" con los integrantes del Comité de Seguridad, los propietarios de los activos, dueños de los subprocesos y la información obtenida de los activos, con los formularios F-1 y F-2, que permiten identificar los controles actuales para las aplicaciones y los controles de seguridad física respectivamente, se determina las posibles amenazas. De este análisis se determina una lista de 30 posibles amenazas que se muestra detalladas en la tabla 4.1.

ÍTEM	AMENAZAS	DESCRIPCIÓN
1	Alteración	Cambio de documentos total o parcial
2	Borrado	Eliminación involuntaria de datos por parte de los usuarios
3	Responsabilidad	Incapacidad de asociar una acción/ transacción a un individuo en concreto
4	Catástrofes naturales	Amenazas ambientales no controlables
5	Copia de datos	Con fines maliciosos o descuido de este medio
6	Cortes de tensión	Suspensión del servicio de energía eléctrica
7	Degradación o pérdida de las redes	Perdida de conexión por volumen de datos transmitidos o por daños
8	Denegación de servicio	Indisponibilidad de los sistemas para los usuarios
9	Dependencia de personal clave	Excesiva dependencia en personal "clave" para la realización de procesos
10	Errores de envió de información	Equivocar el destinatario de la información
11	Errores de usuario	Errores del personal autorizado
12	Fallas de funcionamiento	Indisponibilidad de medios tecnológicos por fallas de componentes de hardware
13	Fallos en el software	Errores humanos de los programadores, funcionamiento incorrecto

ÍTEM	AMENAZAS	DESCRIPCIÓN
14	Fallos técnicos	Fallos por instalación incorrecta de SW ó de configuración
15	Falsificación	Falsificación por medios tecnológicos (phising) o de documentos
16	Falta de seguridad	Amenazas de ambientes físicos no controlables, ejemplo: proveedores, clientes
17	Fuego	Accidente con fuego que afectan el medio de almacenamiento de los activos
18	Ilegibilidad de datos	Información impresa no legible claramente
19	Intercepción enviada por correo físico	Interceptación de información enviada por correo físico
20	Intercepción de datos electrónicos	Interceptación de información que viaja electrónicamente (ejemplo correo electrónico,...)
21	Modificación	Cambio de datos de los registros, falta de información sobre la naturaleza de los cambios sobre los activos
22	Falta de privacidad	Accesos físicos inseguros, sin cerraduras
23	Quiebra del proveedor	Quiebra del proveedor de servicios o bienes de impacto para la empresa
24	Retraso en entrega	Entrega de servicios o bienes fuera de tiempos establecidos
25	Robo	Sustracción o pérdida de soportes de tratamiento de información (papel, portátil, etc)
26	Suplantación de identidad de usuarios	Suplantación de identidad de usuarios (p.e. Acceso no autorizado a usuario y contraseña)
27	Servicio no solicitado o deficiente	Servicio de proveedores deficiente o no solicitado
28	Versiones vulnerables	Versiones con fallas de seguridad
29	Falta de ética	No tiene compromiso con la empresa, comportamiento no ético
30	Virus	Código malicioso

Tabla 4.1 Listado de posibles amenazas a los activos de información

Paso (4) Posibilidad de ocurrencia de las amenazas

Para cada uno de los 28 activos se analizan las 30 amenazas definidas en la tabla 4.1, basado principalmente en la experiencia y el conocimiento de los activos de los participantes de estas sesiones, se define un valor de la escala de 1 a 5, los resultados se muestran en la columna 8 del anexo V.

Paso (5) *Identificación de vulnerabilidades*

Se elabora una lista de las vulnerabilidades existentes que se pueden usar contra aquellos activos que se identificaron como los de mayor impacto para el proceso de Soporte al usuario, el resultado se muestra en la tabla 4.2

Ítem	Vulnerabilidades
1	Acceso lógico no autorizado
2	Control de acceso físico
3	Control de registro de documentos
4	Registro y almacenamiento de datos electrónicos
5	Rotación de personal clave
6	Cumplimiento de políticas y procedimientos
7	Entrenamiento continuo en seguridad
8	Errores de configuración
9	Errores de digitación
10	Errores de procesamiento de aplicaciones
11	Líneas de red de datos desprotegidas
12	Formalización de políticas y procedimientos.
13	Falta de mantenimiento
14	Monitoreo y revisión de logs, herramientas de auditoría
15	Poco detalle o falta de información con proveedores
16	Puertas sin cerraduras, ambientes inseguros
17	Reducción de costos, servicio deficiente
18	Daño de hardware (discos, memorias, tarjetas, etc.)
19	Falla en el suministro de energía o en (UPS, generador, etc)
20	Huracán/terremoto/inundaciones/Erupciones

Tabla 4.2 Vulnerabilidades detectadas

* Una vulnerabilidad es cualquier debilidad que se puede aprovechar

A través de la dinámica de grupos, se define las vulnerabilidades aplicables de la tabla 4.2 para cada amenaza, los resultados se muestran en la columna 9 del anexo V.

Paso (6) *La posible explotación de vulnerabilidades*.

Para las vulnerabilidades detectadas se define el valor en una escala de 1 a 5, de la posibilidad de explotar. Los datos se detallan en la columna 10 del anexo V.

Paso (7) *Estimado del valor de los activos en riesgo*

El riesgo se evalúa contemplando dos elementos básicos: el valor estimado del activo en riesgo y la posibilidad de ocurrencia de que una amenaza aproveche una vulnerabilidad y se produzca un ataque que genera un peligro potencial para la seguridad.

El valor estimado del activo en riesgo es el elemento fundamental para evaluar el riesgo, aquí se determina el daño económico que el riesgo pudiera causar a la organización en relación a la confidencialidad, integridad y disponibilidad, exponiendo a la empresa a posibles pérdida. Los datos se visualizan en la columna 11 del anexo V, que es el valor obtenido de la media aritmética de las columnas 3, 4 y 5.

Paso (8) Posibilidad de Ocurrencia del riesgo

Se obtiene de la media aritmética de la posibilidad de ocurrencia de las vulnerabilidades. Los datos se visualizan en la columna 12 del anexo V

Paso (9) *Valor del Riesgo de los activos*

La evaluación del Riesgo asociado a cada Activo de Información es calculado entendiendo a este; como el nivel de riesgo potencial que estima el propietario del Activo de Información, en función de la *probabilidad* (vulnerabilidad o aplicabilidad de las amenazas) y del *Impacto* en relación a su confidencialidad, integridad y disponibilidad, calculado mediante la siguiente fórmula:

Riesgo = Impacto * Probabilidad

Entendiéndose por *Probabilidad*, la media aritmética de las vulnerabilidades definidas, de acuerdo a la metodología de CLAPAM (Comisión Latinoamericana de Productividad y Medio Ambiente).

Los datos se muestran en la columna 13 del anexo V que se obtiene de multiplicar la columna 11 (valor del activo en riesgo) por la columna 12 (posibilidad de ocurrencia).

4.3 TRATAMIENTO DEL RIESGO

Una vez efectuado el análisis y evaluación del riesgo, para el proceso Soporte al usuario, se realiza la definición de los controles necesarios para mitigar el riesgo potencial.

Se realiza la clasificación de activos de acuerdo al valor del riesgo obtenido para determinar los activos más críticos utilizando la siguiente escala:

0 - 5	Muy bajo
6 - 10	Bajo
11 – 15	Medio
16 – 20	Critico
21 en adelante	Muy crítico

Los resultados de esta clasificación se muestran en la Tabla 4.3

ITEM	ACTIVOS	VALOR DEL ACTIVO EN RIESGO	POSIBILIDADES DE OCURRENCIA DE AMENAZAS	VALOR DEL RIESGO
19	Notebooks (Hw y Sw)	5	2,56	12
26	Software Contable Financiero CAPITAL	5	2,56	12
21	Personal de la empresa de outsourcing que brinda servicios	5	2,50	13
18	Multifuncionales	5	2,33	11
20	Personal interno que da soporte	5	2,33	11
12	Software Contable para servicio de Outsourcing GESTOR	5	2,22	11
17	Líneas telefónicas	5	2,00	9
22	Servicios de IT de proveedores	5	2,00	9
27	Software Control de proyectos WIP	5	2,00	9
23	Servidor de aplicaciones WEB	5	1,90	9
15	Desktop (Hw y Sw)	5	1,89	9
28	Software para Encuesta salarial SIREM	5	1,89	9
4	Informes y reportes impresos o electrónicos	5	1,88	9
14	Centrales telefónicas	5	1,80	8
16	Librerías de respaldo	5	1,80	8
25	Sistema de discos	5	1,80	8
2	DTU	5	1,57	8
6	Servicios de comunicaciones de proveedores	5	1,50	8
10	Servidor de base de datos Oracle	5	1,50	8
13	Switchs	5	1,50	8
7	Servidor de almacenamiento (storage)	5	1,45	7
3	Firewall	5	1,43	7
5	Routers	5	1,43	7
11	Servidor de correo electrónico y BDD de LN	5	1,40	7
24	Servidor de Radius (acceso remoto)	5	1,36	6
8	Servidor de aplicaciones de riesgo	5	1,30	7
9	Servidor de archivos	5	1,30	7
1	Datos del cliente	5	1,25	6

Tabla 4.3 Análisis del riesgo

Considerándose que la selección de objetivos de control y controles del Anexo A de la norma ISO/IEC 27001:2005, se efectuará para los activos desde el rango medio, que se listan a continuación:

1. Personal de la empresa de outsourcing que brinda servicios a Copcil,
2. Software Contable Financiero CAPITAL,

3. Notebooks (Hw y Sw),
4. Software Contable para servicio de Outsourcing GESTOR,
5. Multifuncionales y
6. Personal interno que da soporte

Los otros activos de información no se consideran por que son administrados a través de los contratos de servicios de la empresa de outsourcing de acuerdo a la política de la organización, y su riesgo se considera que ha sido transferido mediante los contratos y los SLAs (Service Layer Agrement) establecidos ó por que de acuerdo a las dimensiones definidas como operacional, regulatorio, financiero, estratégico e imagen no se consideran que tendrían un impacto importante para la organización.

4.4 IDENTIFICACIÓN DE LOS CONTROLES PARA MINIMIZAR EL RIESGO EVALUADO

Un principio básico de cumplimiento de las normas ISO/IEC 27001 y ISO/IEC 17799 es que las organizaciones no deben adoptar todos los controles de seguridad presentados, la clave del cumplimiento es analizar sistemáticamente aquellos controles relacionados al ambiente operacional específico de la organización y justificar si el control es aplicable y apropiado, así también es posible incluir otros controles no referenciados en la norma.

Con base a lo expuesto se realiza el análisis de selección de los controles del Anexo A de la norma ISO/IEC 27001, para modificar el nivel de riesgo evaluado, para los seis activos con mayor riesgo del proceso soporte al usuario. Del cual se obtiene el Enunciado de Aplicabilidad Anexo VI que contiene:

- Los objetivos de control,
- Los controles,
- La justificación para su selección, así como para la exclusión y

- La referencia de la política o procedimiento descritos en los manuales de seguridad y de procedimientos respectivamente.

Se incluye en este anexo para cada uno de los activos un resumen de la brecha de controles actuales y los requeridos por la norma.

4.5 MANUAL DE PROCEDIMIENTOS DE SEGURIDAD

El Manual de Procedimientos para COPCIL está elaborado para cumplir con los requerimientos de la norma internacional ISO/IEC 27001:2005.

Los objetivos básicos que se persiguen al estructurar y establecer el Manual de Procedimientos son:

- Desarrollar los procedimientos de seguridad necesarios para administrar el riesgo potencial de los activos de información, tomando como referencia los controles y procedimientos requeridos en la norma ISO/IEC 27001:2005 para establecer el SGSI.
- Obtener información detallada, ordenada, sistemática e integral que contiene las instrucciones, responsabilidades e información sobre políticas, funciones, sistemas y procedimientos de las distintas operaciones o actividades que se realizan.
- Apoyar en el desarrollo adecuado de las actividades de la empresa, estableciendo responsabilidades, medidas de seguridad, control y objetivos que apoyen el cumplimiento de la función empresarial.

Los procedimientos de gestión establecidos en el Manual de Procedimientos responden a las necesidades de operar el Sistema de Gestión de la Seguridad de la Información y apoyan la implantación de las políticas. Los procedimientos se encuentran documentados en el Anexo VII y son:

NOMBRE DEL PROCEDIMIENTO	CODIGO
Procedimiento para el control de documentos	P-01
Procedimiento para el control de registros	P-02
Procedimiento para la capacitación, conocimiento y capacidad	P-03
Procedimiento para revisiones de la Dirección	P-04
Procedimiento para la realización de auditorias internas	P-05
Procedimiento para la gestión de acciones correctivas	P-06
Procedimiento para la gestión de acciones preventivas	P-07
Procedimiento para la clasificación, archivo, conservación y destrucción de información	P-08
Procedimiento para la administración de cuentas de usuario	P-09
Procedimiento para monitoreo de cuentas de usuario	P-10
Procedimiento para el almacenamiento de archivos	P-11
Procedimiento para la administración de cambios	P-12
Procedimiento para la aceptación de aplicaciones y sistemas	P-13
Procedimiento para compras de software y hardware	P-14
Procedimiento para la administración de incidentes de seguridad	P-15
Procedimiento para la asignación y devolución de computadores	P-16
Procedimiento para la adhesión al sistema de gestión de la seguridad de la información.	P-17

4.5.1 ESTRUCTURA DEL MANUAL DE PROCEDIMIENTOS

El Manual de Procedimientos de COPCIL contempla los siguientes aspectos:

Encabezado: Incluye los siguientes campos: el nombre de la empresa, el Nombre del procedimiento, Revisión, Aprobación, Edición, Página, Código.

Objeto: Permite al lector conocer el fin que se persigue con la gestión del procedimiento.

Alcance: permite al lector identificar a qué aspectos de la norma se refiere el procedimiento y sus límites de aplicación.

Definiciones: aquí se detallan ciertas definiciones a las que regularmente se hacen referencia en el procedimiento, y que son necesarias para interpretar los procedimientos. Identifica y explica el significado de las abreviaturas y siglas utilizadas en el documento.

Referencias: aquí se establecen los documentos de carácter general a los que hace referencia en el procedimiento.

Responsabilidad y autoridad: El designado se encargará de asegurar que el Procedimiento esté implantado, mantenido y de informar al Comité de Seguridad las novedades encontradas.

Descripción: Es un detalle donde se recogen las diversas actividades de la organización, y permite cierto detalle en el conocimiento de las actividades y responsabilidades de quiénes gestionan el procedimiento.

Registros: El campo “anexos” incluye información requerida para la realización del procedimiento, como por ejemplo tablas de datos o información e incluye también los formatos utilizados a lo largo del procedimiento, listas maestras, etiquetas de identificación, etc.

4.6 PROPUESTA DE EVALUACIÓN Y MANTENIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Para realizar un análisis de los controles existentes en la empresa Copcil versus la norma ISO/IEC 27001:2005 se propone la utilización de la Guía de evaluación que se encuentra documentada en el anexo VIII, en la cual se hace referencia a cada uno de los objetivos de control y controles de la norma, así como la descripción de recomendaciones para realizar la verificación del cumplimiento.

El objetivo principal de la guía es identificar las brechas en la estructura actual de control de la empresa y hacer recomendaciones, para la mejora continua del SGSI de manera que se determine y justifique si es necesario o no los controles incluidos en el Anexo A de la norma, sobre la base del análisis y evaluación del riesgo.

Como parte del ciclo PHVA es necesario medir la efectividad de los controles, para verificar que se cumple con los requisitos de seguridad definidos, para realizar esta medición se propone utilizar un conjunto de indicadores detallados en el anexo XI que apoyarán ésta verificación en base al registro de los incidentes en un período determinado que permitirá mantener y mejorar el SGSI.

CAPITULO 5

1 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En la actualidad pocas deben ser las empresas que no se hayan informatizado al menos en forma mínima. En el ámbito doméstico, cada día más son los hogares que cuentan con ordenador y conexión a Internet. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad

- Paralelamente al crecimiento del uso de la informática y de las redes de comunicaciones, se multiplica el número de incidentes de seguridad. Cuanto mayor es el volumen de información procesado y transferido, mayor es el riesgo derivado de su pérdida, alteración o divulgación.

- La seguridad de la información tiene por objetivo proteger a los activos de información de las amenazas a los que están expuestos. La aplicación de medidas de seguridad debe realizarse de manera planificada y racional, para evitar dirigir esfuerzos donde no hace falta o no destinar suficientes recursos donde más falta hace.

- Para que las medidas y mecanismos de protección resulten eficaces, deben integrarse dentro de un sistema más amplio de gestión de la seguridad de la información por que sin un plan director que guíe los esfuerzos de protección de los activos de la organización, por mucho dinero que se invierta en seguridad nunca se alcanzarán niveles satisfactorios.

- Todas las empresas grandes, medianas y pequeñas realizan inversiones en seguridad, según la última encuesta del CSI/FBI realizada en EE.UU.

sobre seguridad y crimen informático correspondiente al año 2006, el 97% de las empresas utilizan antivirus y el 98% también corta fuegos (firewalls). Por tanto, existe consciencia de las amenazas frente a las que hay que protegerse. Con el fin de dirigir eficientemente estos esfuerzos de protección, se vuelve imprescindible realizar un mínimo ejercicio de análisis de riesgos para identificar los activos prioritarios a proteger.

- Los SGSI son capaces de contrarrestar las amenazas a los que se encuentran expuestos los activos de la organización: la información y los elementos hardware y software que la soportan. No se trata de implantar medidas de seguridad, tales como cortafuegos o cifrado de datos porque es la tecnología que está de moda o porque se cree que así se va a estar más seguro. Se trata más bien de evaluar los riesgos reales a los que la información está expuesta y mitigarlos mediante la aplicación de las medidas necesarias y en grado adecuado, con el fin de satisfacer las expectativas de la organización en costo-beneficio.

- No se puede dejar de considerar para las medidas de seguridad el costo de adquisición, mantenimiento y operación, su facilidad de uso, su aceptación entre los usuarios, la percepción de los clientes, su efectividad, etc. Un candado es una medida de seguridad barata, fácil de usar, no requiere mantenimiento ni formación, si es pequeño resulta discreto, es ampliamente aceptado entre los usuarios, pero solamente resultará eficaz en un contexto determinado y para dar satisfacción a un objetivo concreto. Si el contexto o el objetivo cambian, entonces dicha medida de seguridad puede resultar totalmente inadecuada. La mayoría de medidas de seguridad resultan insuficientes si se implantan aisladamente, por lo que deben combinarse con otras. Individualmente solo protegen de ciertas amenazas, mientras que colectivamente protegen un mayor número de amenazas posibles.

- Una de las ventajas de utilizar estándares radica en el hecho de utilizar experiencias de otras organizaciones en beneficio propio, lo que ahorra

tiempo y recursos. Por otro lado, existen regulaciones que recomiendan a las organizaciones basar sus procesos en mejores prácticas de la industria para garantizar el cumplimiento de la ley y para apoyar el cumplimiento de dichas normas, sobre todo en aspectos en los que TI forman parte de la cadena de valor del negocio, así como recomendaciones generadas por auditorías tanto para áreas de TI como para el negocio.

- La Junta Bancaria y la Superintendencia de Bancos y Seguros a través de la Resolución No. JB-2005-834, de 20 de octubre de 2005, dictan normas para la implantación del Riesgo Operativo dentro de las Instituciones del Sistema Financiero Nacional como parte de la preocupación de controlar y administrar el riesgo en este sector.

- La confidencialidad, integridad y disponibilidad de la información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos, por tanto la nueva motivación para llegar a la certificación de la seguridad puede ser una oportunidad de negocio más que un coste.

- El nivel de seguridad alcanzado por medios técnicos demuestra ser limitado e insuficiente por sí mismo, en la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la dirección al frente y se debe considerar también a clientes y proveedores de bienes y servicios.

- Con un SGSI, la organización conoce los riesgos a los que está sometida su información, los asume, minimiza, trasfiere o controla mediante una sistemática definida, documentada y conocida por todos que se revisa y actualiza constantemente. El riesgo se administra ya que no es posible eliminar el riesgo o proteger la información frente a todas las amenazas imaginables.

- Garantizar un nivel de protección total es imposible incluso en el caso de disponer de un presupuesto ilimitado. El propósito alcanzado con el SGSI es gestionar los riesgos de la seguridad de la información de los activos críticos para la empresa Copcil de una forma documentada, sistemática, estructurada, repetible, y adaptada a los cambios que se produzcan en: los riesgos, el entorno y las tecnologías, esto ayuda a dirigir y controlar las actividades de la empresa Copcil en lo referente al proceso Soporte al usuario, pero solo se podrá ratificar esta aseveración el momento en que se implemente el SGSI desarrollado, ya que el alcance del proyecto es el diseño y guía para la implementación.

- La documentación requerida por la ISO 27001 permite estandarizar, controlar, mantener y mejorar continuamente el SGSI, de acuerdo a los cambios de la empresa Copcil y su entorno, no existe documentación requerida en la ISO 17799, ya que más bien constituye una guía de buenas prácticas de los objetivos de control y controles necesarios para lograr la confidencialidad, integridad y disponibilidad de la información.

- La administración de la seguridad de la información para la empresa Copcil es un elemento crítico de éxito y supervivencia, ya que el servicio que presta a sus clientes es principalmente la recepción y generación de información, por tanto la implementación de un SGSI, apoya la diferenciación y permite obtener confianza y reconocimiento de los clientes, la sensación de falta de seguridad no es tan solo una creación artificial, si no que puede generar en falta de motivación para el uso de servicios de outsourcing, que implica la revelación de datos confidenciales como la nómina y la información financiera de los clientes.

- ISO 27001 abarca todos los tipos de organizaciones, dentro de un contexto global del negocio y especifica los requisitos para la aplicación de controles de seguridad de acuerdo a las necesidades de las organizaciones, por lo cual es adaptable a la empresa Copcil.

- A través del análisis de riesgo realizado, se identificó las vulnerabilidades y se definieron los requisitos y objetivos de la seguridad de la información para el proceso Soporte al usuario de la empresa Copcil, los riesgos identificados son administrados a través del SGSI diseñado, el cual además apoya el cumplimiento de las leyes y regulaciones vigentes y mejora el uso de los activos de información.

- Las organizaciones de TI fueron en un principio, enfocadas a temas técnicos, pero conforme ha pasado los años, las organizaciones tienen objetivos dirigidos a la calidad de los servicios por tanto la Gerencia del área de Tecnologías de Información de Copcil consiente del nuevo rol, considera importante el aporte de SGSI como un pilar para cumplir con este objetivo, y así mejorar la calidad de los servicios que ofrecen y la alineación a los objetivos de negocio. Una apropiada administración de las amenazas a los activos de la información, permite que los servicios requeridos por los procesos de negocio estén disponibles cuando se los requiere.

- Actualmente el área de Tecnología de la empresa Copcil dispone de procedimientos no estandarizados ni formalizados, por lo cual la implantación de un SGSI apoyará en forma importante la administración de los activos tecnológicos y el servicio que prestan, en lo referente al proceso Soporte al usuario se identificaron los activos críticos y en ellos se ha enfocado el desarrollo de controles en base a la norma ISO 27001, como el primer paso que debería abarcar a todos los procesos de la empresa..

5.2 RECOMENDACIONES

- En la actualidad existen mucha información disponible pero lo más importante, es la calidad de la información, es decir la exactitud, oportunidad y relevancia de la misma por tanto las organizaciones están

preocupadas por la seguridad de la información y por ello se recomienda la implementación de Sistemas de Gestión de la Seguridad de la Información que son una manera sistemática de manejar la información sensible, que abarcan a personas, procesos y tecnologías de la información.

- Se recomienda a la empresa Copcil no caer en una burocratización del sistema, los procedimientos son solo una herramienta de trabajo muy útil pero no suficiente, la prevención del riesgo para ser efectiva ha de basarse en el compromiso de la dirección y en la confianza de todos los miembros de la organización, al tomar conciencia y comprobar que cumpliendo con el sistema, también se están reduciendo costos considerables y se está generando eficiencia y valor en la actividad empresarial.

- Se recomienda que el Área de Tecnologías de Información de la empresa Copcil, proponga un proyecto de mejoramiento de sus procesos, basado en ITIL, (Information Technology Infrastructure Library) que es una colección de documentos públicos, basados en procesos y en un marco de mejores prácticas de la industria. ITIL tiene que ver con todos aquellos procesos que se requieren ejecutar dentro de las organizaciones para la administración y operación de la infraestructura de TI.

- Se recomienda al Área de Tecnologías de Información continuar con el proceso y obtener la aprobación de la gerencia para los riesgos residuales propuestos y la autorización para implementar y operar el Sistema de Gestión de la Seguridad de la Información propuesto en este trabajo.

- La seguridad de información es un tema amplio y necesario en todas las organizaciones por tanto existe una nueva área de desarrollo para quienes de una u otra manera están involucrados con el control y manejo de información crítica del negocio, se recomienda el estudio a través de organismos especializados y el análisis de otras herramientas disponibles a las normas ISO referenciadas en este documento, que complementan la gestión de IT como COBIT e ITIL.

CONTENIDO

ANEXO I

ORGANIGRAMA DE LA EMPRESA COPCIL CONSULTORA PROFESIONAL CIA LTDA.

ANEXO I
COPCIL Consultora Profesional Cía. Ltda.
Estructura orgánico funcional