

UNIVERSIDAD DE LA HABANA
CENTRO DE ESTUDIOS DE TECNICAS DE DIRECCION

**“BASES METODOLÓGICAS PARA LA ELABORACIÓN
DE UN PLAN DE SEGURIDAD INFORMÁTICA ÚNICO
EN LA EMPRESA CUBANA DE AVIACION S.A.”**

**TESIS PRESENTADA EN OPCIÓN AL TÍTULO ACADÉMICO
DE MÁSTER EN DIRECCIÓN**

Autor:

Lic. Andrés Avelino Martínez Morales

Tutor:

Dr. C. Luis Barreiro Pousa

La Habana, Marzo 2016

DECLARACIÓN DE AUTORÍA

Yo, **Andrés Avelino Martínez Morales** declaro que el trabajo que presento como Tesis de la Maestría en Dirección, titulado **Bases metodológicas para la elaboración de un plan de seguridad informática único en la empresa Cubana de Aviación S.A.** es original, fruto de la relación de trabajo científico con mi tutor y autorizo al Centro de Estudios de Técnicas de Dirección de la Universidad de La Habana para que haga uso del mismo con fines docentes.

Para que así conste firmo la presente a los 31 días del mes de marzo de 2016.

Firma del autor

AUTORIZACIÓN DE DEFENSA

Yo **Dr.C. Luis Barreiro Pousa**, tutor de la tesis de Maestría en Dirección titulada **Bases metodológicas para la elaboración de un plan de seguridad informática único en la empresa Cubana de Aviación S.A.**, del maestrante **Andrés Avelino Martínez Morales**, declaro que he realizado la última revisión de la tesis y considero que posee los requisitos necesarios para su defensa, por lo que solicito al Comité Académico de la Maestría que convoque el tribunal de defensa correspondiente.

Para que así conste, firmo la presente a los 31 días del mes de marzo de 2016.

Firma del tutor

A los que siempre han confiado en mí.

Agradecimientos.

A todos mis familiares y amigos, que han compartido conmigo momentos de trabajo, dejaciones y sacrificios, pero también de amor, felicidad y alegría, me han brindado siempre apoyo y han sido comprensivos y colaboradores.

Al Dr. Luis Diego Méndez García por sus consejos y observaciones. Por los años de trabajo juntos en una actividad tan compleja y, en ocasiones, ingrata.

Al Centro de Estudios de Técnicas de Dirección, su claustro de profesores y trabajadores administrativos.

A mi tutor, Dr. Luis Barreiro Pousa, por sus valiosas orientaciones y el apoyo prestado.

A todos mis compañeros.

Resumen.

La información en las empresas constituye un activo sensible, siendo un objetivo mantenerla a resguardo de cualquier amenaza que pueda ponerla en riesgo. De ahí la necesidad de protegerla, lo que se logra con una adecuada planificación de su seguridad, actividad compleja al estar involucradas personas y sistemas informáticos.

La seguridad informática es la encargada de buscar los mecanismos para proteger la información que se gestiona con las TICs, enfocándose en la protección de la infraestructura computacional y todo lo relacionado con esta. El instrumento que utiliza para ello, es el Plan de seguridad informática, en el que se describen políticas, medidas y procedimientos para una gestión segura de las TICs y la información.

La complejidad de la gestión de la empresa Cubana de Aviación S.A. y la alta dispersión geográfica que presenta en su ubicación física, constituyen una singularidad que caracteriza la planificación de la seguridad de sus activos informáticos, siendo un imperativo disponer de una herramienta que permita planificar, de manera estándar y eficiente, la seguridad de estos.

En el presente trabajo se presenta una propuesta de Bases metodológicas para la elaboración de un Plan de seguridad informática único para la empresa, partiendo de sus necesidades y las características de su gestión.

Palabras claves: planificación, seguridad, seguridad informática, políticas de seguridad, tecnologías de la información y las comunicaciones, TIC, confidencialidad, integridad, disponibilidad.

Índice.

DECLARACIÓN DE AUTORÍA	i
AUTORIZACIÓN DE DEFENSA	ii
Agradecimientos.	iv
Resumen.	v
Introducción.	1
Capítulo I. La gestión de la seguridad de la información en las organizaciones.	10
1.1 La información para las organizaciones.	10
1.2 Las Tecnologías de la información y las comunicaciones en los procesos de las organizaciones.	16
1.3 La seguridad de la información y la seguridad informática.	19
1.4 El Plan de Seguridad Informática.	27
1.5 Normatividad para la Gestión de la Seguridad Informática.	31
Capítulo II. Planificación de la seguridad informática en Cubana de Aviación S.A.	35
2.1 Evolución de la empresa Cubana de Aviación S.A.	35
2.2 Caracterización del Sistema Informático.	39
2.3 Problemas en la planificación de la Seguridad Informática.	53
Capítulo III. Bases metodológicas para la confección de un Plan único de Seguridad Informática.	61
3.1 Propuesta de solución para la planificación de la Seguridad Informática.	61
3.2 Guía para la elaboración de un PSI único.	63
3.3 Proceso de planificación de la seguridad informática.	74
Conclusiones.	80
Recomendaciones.	82
Bibliografía.	83
Anexos.	89
Anexo 1 Serie ISO/IEC 27000.	89
Anexo 2 Legislaciones más significativas en el contexto legal cubano referente a al uso de las tecnologías de la información y las comunicaciones y la información que en ellas se gestiona.	91
Anexo 3 Ubicación geográfica de las entidades que componen Cubana de Aviación S.A.	94
Anexo 4 Mapa de procesos CU	98

Anexo 5 Análisis de la situación actual (agosto 2015) en las tecnologías de la información y las comunicaciones en Cubana de Aviación S.A. (Matriz DAFO).....	99
Anexo 6 Relación de dependencias administrativas pertenecientes a Cubana de Aviación S.A. en el territorio de la República de Cuba y en el exterior	110
Anexo 7 Políticas establecidas para el Sistema de Gestión de Seguridad de la Información (SGSI).	116

Introducción.

Las empresas actuales son un buen ejemplo de la diversidad de uso y posibilidades de las Tecnologías de la Información y las Comunicaciones (TIC), encontrándose automatizados desde procesos contables, hasta complejos procesos productivos, dirigidos totalmente por robots o autómatas informáticos.

Durante mucho tiempo las TICs fueron vistas como un elemento aislado de la organización, consumiendo grandes presupuestos y con un alto nivel de incumplimiento. Según Roach (1987), fueron cuestionadas en su momento por falta de productividad y para Carr (2003) por su falta de importancia en la organización. Sin embargo, hoy en día, el entorno cada vez más cambiante y globalizado demanda de las compañías acciones ágiles e innovadoras para elevar su nivel de competencia, lo que ha dado a las TICs un papel fundamental en la toma de decisiones de los directivos, siendo cada vez son más usadas para el apoyo y automatización de todas las actividades de la empresa.

Gracias a ellas, las organizaciones han conseguido obtener importantes beneficios, entre los que se pueden mencionar la mejora de sus operaciones; la posibilidad de llegar a una mayor cantidad de clientes; la optimización de sus recursos; la apertura a nuevos mercados; un conocimiento más profundo de las necesidades de los clientes, lo que permite brindar un servicio personalizado de mejor calidad y lograr una comunicación más fluida con empleados, clientes y proveedores. En pocas palabras, las TICs permiten aumentar considerablemente la eficiencia y la eficacia. En la actualidad, expresa Porter (2006), se considera que las TICs aportan valor a las organizaciones hasta el punto de proporcionar ventaja competitiva.

Estas posibilidades que brindan las TICs se logran a partir de la acumulación y organización de los datos que se obtienen por variadas fuentes, así como por el uso y gestión de estos y las tecnologías que los soportan, para obtener información relacionada con el objeto de la entidad y que se puede considerar con cierto grado de confidencialidad, al ser datos relativos a personas u organizaciones y es preciso que esté disponible en el momento que se necesita, solicitada por los autorizados a hacerlo

y que no haya sido manipulada. Es un objetivo, entonces, protegerla ante cualquier amenaza que pueda ponerla en riesgo y, de ahí, la necesidad de establecer mecanismos de seguridad para lograr este objetivo.

La expansión de máquinas enlazadas en red y la necesidad de compartir información y recursos, tratando de disminuir trámites burocráticos y acortando tiempos de respuestas, llevó al crecimiento acelerado de una red global, Internet, al aumentar las redes que se interconectaban, a la par que aumentaba el auge de la informática de consumo con la expansión de las computadoras personales y su inclusión en la vida personal diaria. Este crecimiento y desarrollo de las TICs fue imponiendo la necesidad, cada vez mayor, de orden y control en su uso para lograr una correcta gestión de estas y la información que contienen.

Sin embargo, no fue hasta 1988 que se tomara en serio el tema de la seguridad de las TICs, con el primer gran incidente relacionado con la seguridad informática, la aparición del primer virus informático, el famoso *worm* o gusano de Internet¹, que provocó que miles de computadoras conectadas a la red se vieran inutilizadas durante días, con pérdidas que se estimaron en millones de dólares. Desde ese momento el tema de la seguridad en los sistemas operativos y las redes ha sido un factor a tener en cuenta por los administradores de sistemas informáticos.

En el contexto del desarrollo de las TICs, se esperan resultados rápidos y con bajo costo, pero esto va en detrimento de lo seguro. Lograr una seguridad confiable es una actividad compleja al estar involucradas personas y las cosas que conocen, sus relaciones con otras personas y con los sistemas informáticos y por ser las computadoras complejas, inestables y estar plagadas de errores (Schneider, 2004). Los sistemas de hoy en día se encuentran bajo amenaza constante por los errores humanos y los fenómenos naturales, así como por ataques de diferente índole como

¹ El gusano Morris fue el primer ejemplar de malware autor replicable que afectó a Internet, entonces ARPANET. El 2 de noviembre de 1988, aproximadamente 6 000 de los 60 000 servidores conectados a la red fueron infectados por este gusano informático, lo que motivó que DARPA creara el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés) en respuesta a las necesidades expuestas durante el incidente. Erradicarlo costó casi un millón de dólares, sumado a las pérdidas por haberse detenido casi toda la red, siendo estimadas las pérdidas totales en 96 millones de dólares, cifra significativa en aquel momento.

los virus informáticos, los hackers y el espionaje corporativo, todos buscando explotar vulnerabilidades.

Solo con una información gestionada de manera segura y confiable se puede garantizar el éxito de la empresa. La seguridad informática es la encargada de buscar los mecanismos para proteger la información que se gestiona con las TICs, enfocándose en la protección de la infraestructura computacional y todo lo relacionado con esta. El instrumento que utiliza para ello, es el Plan de seguridad informática (PSI), en el que se describen políticas, medidas y procedimientos para una gestión segura de las TICs y la información.

A pesar de las ventajas de un modelo operativo basado en la infraestructura tecnológica que ofrecen las TICs, las organizaciones corporativas enfrentan un alto riesgo al incrementar sus relaciones con múltiples socios, procesos, sistemas, regulaciones y políticas, lo que se une al intercambio de datos, sistemas compartidos y la presencia de ejecutivos en localidades remotas con necesidades de información.

Las regulaciones gubernamentales siempre han sido parte de los negocios. Hoy en día lineamientos de este tipo inciden prácticamente en todo, desde la ubicación de oficinas y centros de cómputo con su equipamiento activo, hasta el contenido y ubicación de la información del negocio. Los escándalos financieros han impulsado a ello. Han surgido reglas estrictas para tratar de garantizar transparencia, responsabilidad y gobierno. Nuevas legislaciones sobre intercambio de información y privacidad se derivan de lo fácil que puede resultar extraer y transferir información crítica, ya sea por error o de manera intencional. Garantizar la seguridad de bienes, personas, información e infraestructura es un reto para las organizaciones.

El concepto de seguridad ha tomado un nuevo significado. Seguridad era sinónimo de mantener los activos a salvo. Ahora, significa mantener el negocio a través de cualquier crisis, desde una pequeña hasta una con proporciones catastróficas y para ello es preciso definir determinadas reglas, de manera que sea posible poder dar seguimiento al camino que sigue la información desde su origen hasta su destino, en cualquier transacción que se realice, dejando la trazabilidad necesaria que permita recorrer este

camino en sentido contrario, buscando, en caso de algún incidente, las causas y sus autores.

La alta dependencia de los procesos de las empresas de las TICs, ha posibilitado que se comiencen a ver a estas tecnologías como elemento activo en todas las fases de la vida de la organización, surgiendo así una fuerte relación entre las estrategias de la empresa para llevar sus negocios y la infraestructura TICs y su seguridad, por lo que en el ámbito empresarial ha surgido un conjunto de regulaciones y normas para la administración de las TICs, consideradas como buenas o mejores prácticas y que constituyen principios a seguir desde el alto nivel, facilitando una buena toma de decisiones. Es importante la adecuación de estas regulaciones y normas al contexto de la organización.

En Cuba, desde hace varios años y cada vez con más fuerza, las TICs se han ido generalizando y son innumerables las aplicaciones de que se dispone en disímiles campos de las investigaciones, la producción y los servicios. A tono con los cambios en el modelo económico cubano, se ha planteado la necesidad de ordenar todo lo relacionado con las TICs y se puede apreciar, en los Lineamientos del VI Congreso del Partido, aprobados en abril de 2011, la voluntad política de la dirección del país de avanzar en la estrategia de uso de las TICs, pese a la crisis internacional y el bloqueo, al existir 6 Lineamientos relacionados con la temática. En específico 3 de ellos, los Lineamientos 135, 223 y 228 están dirigidos a fortalecer las capacidades de vigilancia tecnológica y llaman a fortalecer la seguridad.

De igual forma, en la Primera Conferencia Nacional del Partido, celebrada en enero de 2012, se aprobó el *objetivo 52*, que plantea: *"Aprovechar las ventajas de las tecnologías de la información y las comunicaciones, como herramientas para el desarrollo del conocimiento, la economía y la actividad política e ideológica; exponer la imagen de Cuba y su verdad, así como combatir las acciones de subversión contra nuestro país."*

Cubana de Aviación S.A. (CU), línea bandera de Cuba, como componente del sistema empresarial cubano, está llamada a revisar su funcionamiento, en consonancia con

estos Lineamientos. Su misión es el transporte de pasajeros, carga y correo en el territorio nacional, así como hacia y desde el exterior. Su gestión de operaciones es altamente compleja, al tener dependencias en prácticamente todo el país, además de 22 gerencias en 20 países y gran cantidad de procesos para su funcionamiento, características distintivas, con alta incidencia en la infraestructura de las TICs, condicionando el empleo de redes de diferente tipo y el uso de un alto número de sistemas y aplicaciones complejas y con alta demanda de accesos a los mismos para el intercambio de datos, obligando a una vigilancia constante sobre la infraestructura de TICs que soporta todo el procesamiento e intercambio de información, como garantía de que ésta sea confiable y oportuna.

La expansión territorial de CU provoca la existencia de gran variedad de áreas de trabajo y locales físicos, con una considerable cantidad de activos informáticos dispersos en todo el país y en el exterior, todos sometidos a diferentes circunstancias, en dependencia de las características del lugar, lo que provoca una alta variedad de amenazas a las TICs y a la información a que da soporte.

Esto implica que la organización esté constantemente amenazada por factores de distintos tipo, como los fenómenos naturales, las negligencias y los errores de operación, exponiendo a riesgos los sistemas y la confidencialidad, la integridad y la disponibilidad de la información contenida en ellos, obligando a tener un número elevado de medidas de prevención, detección y enfrentamiento a las amenazas para garantizar la seguridad.

La expansión territorial que caracteriza a la empresa, implica que sean elaborados PSI para cada área física diferente, en los que se encuentran identificadas y enunciadas las medidas para la gestión de la seguridad. Cada uno de estos PSI presenta acciones para enfrentar vulnerabilidades y minimizar los riesgos, existiendo diversidad de soluciones para problemas similares, diferentes interpretaciones de determinadas situaciones, enfoques contradictorios de problemas y diversidad de criterios respecto a un mismo tema, provocando el desconocimiento de directivos y trabajadores de sus

responsabilidades y modos de actuación y el planteamiento de disímiles respuestas a violaciones de índole similar.

Esto, entre otras dificultades, provoca que no sea posible una gestión de la seguridad de las TICs adecuada y estándar para todas las partes componentes de la organización, al dificultarse la planificación del enfrentamiento de las dificultades y el seguimiento de los planes que se elaboran para ello. Es decir, se presenta la dificultad de que la planificación de la seguridad informática en Cubana de Aviación S.A. no responde a sus necesidades como organización.

Partiendo de lo anterior, se presenta el problema científico ¿Cómo asegurar que la planificación de la seguridad informática en Cubana de Aviación S.A. responda a sus características?

Constituyendo el objeto de investigación el Sistema de Planificación de Seguridad Informática en la empresa Cubana de Aviación S.A.

El objetivo general de la investigación es estructurar un plan único de seguridad informática para Cubana de Aviación S.A.

Constituyendo objetivos específicos:

- Identificar el conjunto de regularidades y normas que constituyen la base de organización de las TICs y de la gestión de su seguridad.
- Realizar un diagnóstico sobre la planificación de la seguridad de las TICs y su uso en Cubana de Aviación S.A.
- Definir las bases metodológicas para la confección de un plan único de seguridad informática.

Para ello, las preguntas científicas que se tuvieron en cuenta a lo largo de la investigación fueron:

1. ¿Existen en Cubana de Aviación S.A. condiciones para la gestión adecuada de la seguridad de la información?

2. ¿Cuáles son las dificultades actuales que enfrenta Cubana de Aviación S.A. relacionadas con la planificación de la seguridad informática?
3. ¿Cuáles son las regulaciones y normas relacionadas con la seguridad de las tecnologías aplicables a la organización?
4. ¿Es posible contar con un único documento para gestionar la seguridad informática en todas las dependencias de la empresa?

Y para ello se desarrollaron las siguientes tareas científicas:

1. Revisión de los documentos existentes para la adopción de medidas inherentes a la seguridad de las TICs.
2. Evaluación de diferentes tendencias en el estado del arte de la seguridad informática que puedan ser asumidas como buenas o mejores para su aplicación en Cubana de Aviación S.A.
3. Realizar un diagnóstico de la situación actual de Cubana de Aviación S.A. respecto a las TICs y su uso y la planificación de la seguridad informática.
4. Definir los elementos que constituyen las bases metodológicas para elaborar un plan único para la gestión de la seguridad informática en Cubana de Aviación S.A.

La investigación se realizó bajo un enfoque fundamentalmente cualitativo, mediante acciones descriptivas y explicativas, utilizando métodos empíricos y teóricos. No se conforma ningún escenario, sino que se observan los existentes.

Los métodos empíricos abarcaron:

- La observación en su variante de análisis de documentos, como planes de seguridad informática, informes, legislaciones y trabajos realizados por estudiosos del tema.
- La observación participante, mediante el análisis de situaciones y la exploración de información existente, la manera en que se enfoca la actividad de planificación de la seguridad informática y los conocimientos que poseen los implicados en este proceso.

- Entrevistas, realizadas a directivos y trabajadores, todos usuarios de las tecnologías de la información y las comunicaciones, para una mejor percepción de la situación actual y las perspectivas de futuro, así como las proyecciones existentes y diferentes opiniones en torno a lo relacionado a la seguridad informática dentro del entorno de la empresa.
- El trabajo en grupo para la recopilación y procesamiento de información de interés y base del diagnóstico, el análisis de situaciones y la definición de los pasos a seguir.

Los métodos teóricos comprenden:

- El análisis histórico lógico como forma de conocer el fenómeno objeto de estudio, desde su surgimiento y desarrollo, para establecer la interrelación entre la planificación de la seguridad informática y otros aspectos que intervienen en la gestión de la empresa para el cumplimiento de su misión.
- El análisis y la síntesis para el estudio de la bibliografía asociada, a los efectos de establecer los fundamentos teóricos de la investigación que permitan precisar conceptos y teorías, generalmente aceptados, sobre el tema.
- La inducción y deducción para la conclusión de ideas y adopción de resultados.

Todo bajo un enfoque sistémico que permitió el movimiento iterativo sobre la información recopilada.

No existen antecedentes de este tipo de estudio en otras empresas cubanas, por lo que el resultado tiene novedad científica.

El informe está estructurado en 3 capítulos, abarcando, cada uno, los siguientes aspectos:

Capítulo I. La gestión de la seguridad de la información en las organizaciones. En el que se aborda todo lo relacionado con conceptos y argumentos que fundamentan el tema y las legislaciones y normas que existen referentes a esta temática.

Capítulo II. Planificación de la seguridad informática en Cubana de Aviación S.A.

En el que se abordan los elementos que inciden en la situación problemática y se determina el conjunto de actividades, hechos o situaciones que constituyen vulnerabilidades, desde el punto de vista de la planificación de la seguridad de las tecnologías y de la información.

Capítulo III. Bases metodológicas para la confección de un Plan único de Seguridad Informática.

En el que se enuncian las bases metodológicas para la conformación de un único PSI para toda la empresa y se presenta una guía que describe los pasos a seguir para la confección del mismo, de acuerdo al análisis de las diferentes características y condiciones de Cubana de Aviación S.A. en el uso de las tecnologías de la información.

Capítulo I. La gestión de la seguridad de la información en las organizaciones.

1.1 La información para las organizaciones.

La información es inherente al ser humano. La necesita para satisfacer su curiosidad y conocer el entorno que le rodea. La sociedad basa su desarrollo en el conocimiento y dominio de este entorno y, las organizaciones, como elementos componentes de esta, precisan la información para el cumplimiento de sus objetivos.

La información constituye un elemento importante para todas las personas, jurídicas o naturales. Para las empresas es uno de los activos más importantes con los que cuenta. Es necesaria para poder tener visión cronológica de sucesos y acontecimientos que constituyen la historia de cualquier entidad, revivir escenarios, evaluar hechos y hacer análisis para llegar a conclusiones respecto a lo acontecido, enriquecer el conocimiento de la propia organización y poder decidir los siguientes pasos, es decir, de ella depende las decisiones que se toman y por tanto las acciones futuras a seguir y que determinan el curso de la vida.

El incremento de la competencia a nivel mundial ha originado una creciente necesidad de técnicas de captación y análisis de información sobre el entorno competitivo y tecnológico y, en particular, de formas organizativas y herramientas que faciliten dicho objetivo con el propósito de reducir la incertidumbre en la toma de decisiones y realizar una planeación con un mayor grado de certeza.

La toma de decisiones es el proceso mediante el que se define un problema, se recopilan datos, se generan alternativas y se selecciona un curso de acción (Hellriegel & Slocum, 2004). Es un proceso para identificar y seleccionar una acción para resolver un problema específico (Stoner, 2003). La importancia de la información en la toma de decisiones queda latente en la definición de decisión como proceso de transformación de la información en acción (Forrester, 1968) (*Figura 1*).

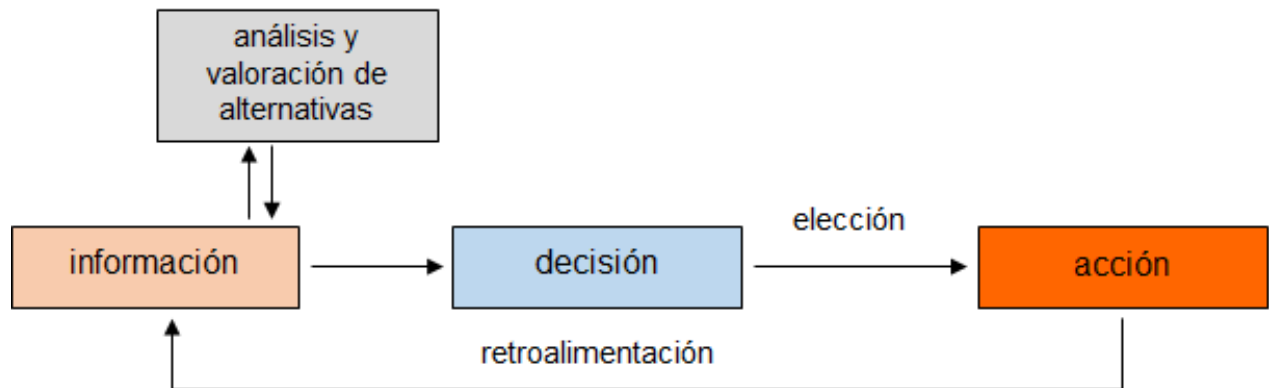


Figura 1. Proceso de toma de decisiones

Fuente: elaboración propia

Los datos son “secuencia de hechos en bruto y representan eventos que ocurren en las organizaciones o en el entorno físico antes de ser organizados y ordenados en una forma que las personas puedan entender y utilizar.” (Laudon & Laudon, 2004, p.8). Aislados no tienen sentido en sí mismos, es preciso el procesamiento adecuado y teniendo en cuenta un contexto, para ser utilizados. Son la mínima unidad semántica y se corresponden con elementos primarios que por sí solos son irrelevantes como apoyo a la toma de decisiones. Se pueden ver como un conjunto discreto de valores, que no dicen nada sobre el porqué de las cosas y no son suficientes para la acción.

La información “es el resultado de haber organizado o analizado los datos de alguna manera y con un propósito.” (Stoner, Freeman & Gilbert Jr., 1996, p.672), es decir, la información “son los datos que se han moldeado en una forma significativa y útil para los seres humanos.” (Laudon & Laudon, 2004, p.8).

La información comprende los datos y los conocimientos que se usan en la toma de decisiones (Ferrell & Hirt, 2004) y siempre está presente en las organizaciones, “no hay organizaciones sin información, lo que existen son organizaciones desinformadas” (Horton, 1985, p.43). Con ella se reduce la incertidumbre o aumenta el conocimiento sobre algo, es un conjunto de datos con un significado, un mensaje en determinado contexto, disponible para uso inmediato, proporcionando orientación a las acciones, por el hecho de reducir el margen de incertidumbre con respecto a las decisiones

(Chiavenato, 2006). Mientras más informado se esté sobre determinado aspecto, más acertadas serán las decisiones que se tomen respecto al mismo.

Estos autores coinciden en valorar que la información resulta de vital importancia para la organización. Pero para llegar a ser información útil, es preciso que los datos sean procesados y acomodados, de forma tal que tomen valor, que adquieran significado, aportando confianza a la misma y para ello es necesario que sea de calidad, es decir, oportuna, suficiente y relevante, con un engranaje tal, que garantice la adquisición del conocimiento necesario para el desarrollo de la organización, aportando retroalimentación para mejorar la entrada de datos. La información es, entonces, conocimientos basados en los datos, a los cuales, mediante un procesamiento, se les ha dado un significado, un propósito y una utilidad y en un determinado contexto, sirven para disminuir la incertidumbre y aumentar el conocimiento sobre un tema específico.

Datos, información y conocimiento son elementos fundamentales para la toma de decisiones en las organizaciones, pero su significado no es tan evidente y sus límites no siempre son claros. Estos tres elementos forman un sistema jerárquico de difícil delimitación (Díaz Duarte, 2005). Lo que significa dato para un individuo puede significar información o conocimiento para otro y viceversa, lo que provoca confusiones, de ahí la importancia de dejar establecido cómo se relacionan y los aspectos que los diferencian.

El proceso relacionado con la obtención de información tiene implícito un conjunto de momentos importantes que permiten dar significado a los datos captados:

La información son datos que adquieren un mayor significado luego que se codifican y se transmite en un lenguaje comprensible para el usuario. Para que los datos se conviertan en información es necesario la:

- Captación: Implica asimilar el dato primario, que debe reflejar un hecho real. Se representa por medio de símbolos de un lenguaje previamente determinado.

- Asimilación: Es similar, pero se produce cuando el dato se obtiene de una base de datos u otra fuente.
- Transmisión: Envío de datos a los lugares donde se utilizará.
- Almacenamiento: Conservación del dato en archivos o bases de datos de diferentes tipos.
- Asociación: Relación de un dato con otro para conferirle más capacidad informativa.
- Cálculo: Operaciones matemáticas que se realizan sobre los datos para conferirle más valor informativo. Implican suma, resta, clasificación u ordenamiento.
- Consulta: Búsqueda en los archivos o base de datos, con arreglo a un determinado criterio, para poder utilizar los datos almacenados en la solución de un problema.
- Distribución: Entrega de la información procesada.

(Blanco Encinosa, 2001, p.81)

Es decir, el proceso de adquisición del conocimiento constituye un sistema, formado, por un “conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.” (Laudon & Laudon, 2004, p.9).

Para procesar los datos de la organización y transformarlos en información, es fundamental un Sistema de Información (SI).

“Las empresas necesitan diferentes tipos de sistemas de información para apoyar la toma de decisiones y manejar actividades de diversos niveles y funciones organizacionales.” (Laudon & Laudon, 2004, p.9). Un sistema de información administrativa es un mecanismo de ordenación formal que “permite poner a disposición de los gerentes la información exacta y oportuna que necesitan para un proceso de toma de decisión más fácil, así como para efectuar con eficacia las funciones de planificación, control y operaciones de la organización” (Stoner, Freeman & Gilbert Jr.

1996, p.672), es un sistema que “proporciona a la gerencia la información que necesita, a intervalos periódicos.” (Robbins & Coulterlo 2006, p.618)

Estas definiciones tienen en común el concepto de que un SI de la empresa debe proporcionar a la gerencia información útil para la toma de decisiones y el control, debiendo estar al servicio de su enfoque de negocio y abarcando tres elementos o niveles bien definidos: la gerencia estratégica de la organización, la toma de decisiones y los procesos administrativos internos.

El proceso de toma de decisiones tiene en la información su materia prima. Esta es fundamental, ya que sin ella no resultaría posible evaluar las opciones existentes o desarrollar nuevas. En las organizaciones que se encuentran sometidas constantemente a la toma de decisiones, la información adquiere un rol fundamental y, por ello, un valor inigualable.

Tres elementos básicos caracterizan a la información: la confidencialidad, la integridad y la disponibilidad, entendiéndose como tal, la garantía de confianza recíproca entre el que la entrega y el que la recibe, que no carece de ninguna parte respecto al momento de su captación y que está lista para utilizarse en cualquier momento (ISO/IEC 27001, 2005) (Resolución 127 MIC, 2007) (Misfud, 2012).

La **Figura 2** muestra, de manera general, el proceso de obtención de la información. Este proceso, como sistema en sí, cuenta con su entrada y su salida bien definidos, con un flujo entre una fuente y un destino. Los datos son adquiridos, por diversas vías, pasando a una etapa de tratamiento, que incluye la transformación, el almacenamiento y registro de estos, siendo entregados, en forma de información, con un valor determinado, proporcionando, a su vez, una retroalimentación al sistema, mediante mecanismos de control que monitorean su desempeño, garantizando las correcciones necesarias para el logro de los objetivos planteados.

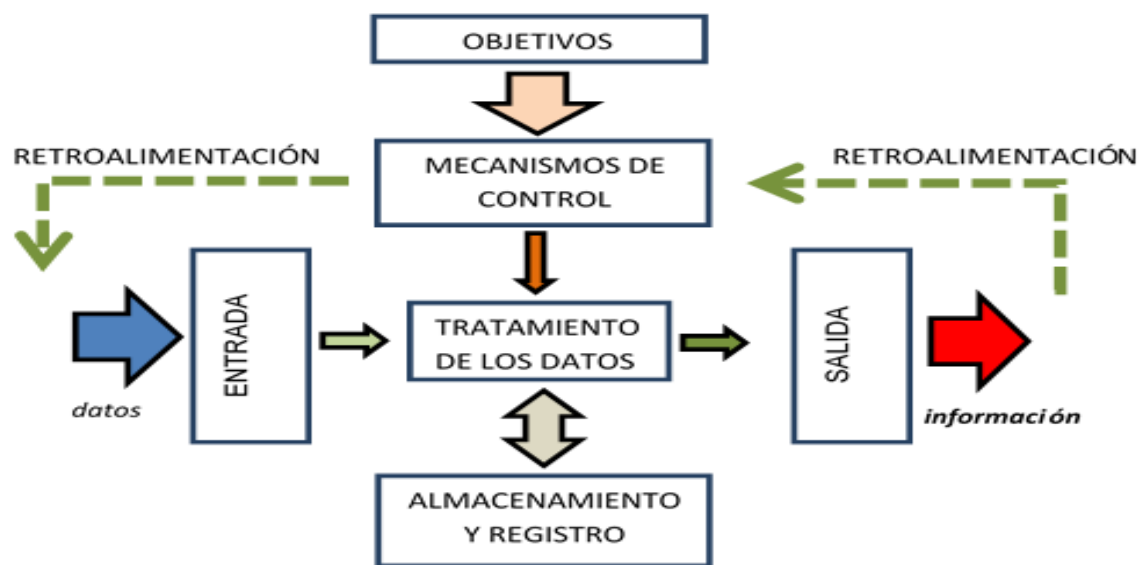


Figura 2. El Proceso de obtención de Información

Fuente: elaboración propia

Las organizaciones necesitan gestionar la información que poseen. Los datos, fuente de la información, deben ser captados periódicamente para mantenerlos actualizados. El entorno y las influencias diversas que recibe, pueden provocar que los datos sufran variaciones necesarias para adecuarse a las condiciones del momento y que influyan en los resultados finales del tratamiento que reciben. De esta manera, la información estará atemperada con el momento.

Un aspecto de gran importancia en los SI es el flujo informativo, fundamental para un correcto diseño de este y que debe garantizar que la información pueda circular en todos los sentidos, ascendente, descendente, horizontal y transversal y contener informaciones tanto internas como externas, brindando, en cada paso, los elementos necesarios para el funcionamiento estable y adecuado de la organización y sus procesos.

A la información le es intrínseco valor histórico, constituyendo parte importante de la cultura de las entidades, de su memoria, de ahí la necesidad de que sea almacenada de manera organizada para poder disponer de ella cuando sea necesaria.

A lo largo de la historia, la forma de almacenamiento y acceso a la información ha ido variando. En la Edad de Piedra el hombre plasmaba en las paredes de las cuevas que

habitaba, mediante dibujos y símbolos, los hechos y acontecimientos que consideraba importantes y necesarios preservar. En la Edad Media, el principal acervo se encontraba en las bibliotecas que se armaban, funcionaban y se conservaban en los monasterios. A partir de la Edad Moderna, gracias al nacimiento de la imprenta, los libros comenzaron a fabricarse en serie y surgieron los periódicos. En el siglo XX aparecen los medios de comunicación masiva como la televisión, la radio y la telefonía, con un desarrollo vertiginoso, llegando a los medios y herramientas digitales actuales y que constituyen verdaderos almacenes de datos e información.

El propio hecho de almacenar la información para poder disponer de ella cuando se le necesite, implica la necesidad de protegerla, o sea, guardarla de manera que se evite su deterioro o pérdida. Hasta hace unos años era almacenada en papel, cintas de celuloide o audio y otros soportes similares, por lo que toda su seguridad se limitaba a la seguridad física del local en que se almacenaba el soporte que la contenía, es decir, la preservación documental. Datos de clientes y proveedores de la organización, de empleados, estadísticas de comportamiento de mercados, resultados económicos, estrategias futuras, *know-how* de productos y servicios, entre otros, quedaban registrados en papel o cintas, con todos los problemas que acarrea el almacenaje, transporte, acceso y procesado, además del deterioro obligado de estos soportes informativos.

1.2 Las Tecnologías de la información y las comunicaciones en los procesos de las organizaciones.

Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de elementos y medios técnicos y la manera de comunicarse entre ellos, desarrollados para gestionar información y su disseminación. Constituyen el soporte por excelencia de los SI. Abarcan un abanico de soluciones muy amplio. Incluyen tecnologías para almacenar información y recuperarla después, enviarla de un sitio a otro y procesarla para obtener resultados. En la actualidad, las organizaciones operan o centran gran parte de su actividad en estos recursos, agrupados en redes que facilitan el procesamiento y la disseminación de la información.

Las TICs han revolucionado la manera hacer negocios en el mundo. El surgimiento de Internet ha permitido la expansión de los negocios a nivel internacional porque reduce la distancia entre mercados, especialmente en términos de intercambio de información. El surgimiento del comercio electrónico, el fácil acceso a cadenas internacionales de suministros y a las redes de producción y distribución por medio de Internet, impulsa a muchas empresas a reasignar sus recursos hacia la producción de exportaciones (Solórzano, 2006). El uso de Internet también ofrece nuevas oportunidades de publicidad, permite que las compañías estén más visibles y sean más fáciles de contactar por parte de los clientes actuales y futuros.

En el artículo “Cómo obtener ventajas competitivas por medio de la información” (Porter & Millar, 1985) se señala que la tecnología de la información ha logrado llegar a todos y cada uno de los puntos de la cadena de valor, transformando la manera en que se realizan las actividades de producción de valor y la naturaleza de los enlaces entre ellas, efectos básicos que explican el que las TICs hayan adquirido un valor estratégico y que sea diferente de otras tecnologías que emplean las empresas. En la actualidad, el carácter del progreso tecnológico se ha invertido, la tecnología de la información avanza más deprisa que las tecnologías de tratamiento de lo físico.

Las TICs evolucionan de forma rápida, siendo cada vez más importante el impacto estratégico de estas sobre la operatividad de las organizaciones, así como la gestión adecuada de las mismas (Benemati et al., 1997), por lo que se tipifica el rol de las TICs en una organización como el ajuste o alineamiento con los objetivos estratégicos de la organización (Olugbode et al., 2007). Las TICs únicamente pueden estar bien alineadas si la infraestructura que se ha utilizado para implementar la estrategia de la organización es la adecuada. Por ello, la estrategia de las TICs debe dar soporte tanto a la estrategia de la organización, como a los procesos de negocio de la misma.

Los beneficios que proporcionan las TICs se manifiestan en un mejor aprovechamiento del tiempo al poder automatizar tareas rutinarias y una mejor gestión mediante el uso de aplicaciones y dispositivos para el control de los procesos del negocio. Mejoran el rendimiento empresarial y su uso supone un importante ahorro de tiempo y recursos, al

simplificar y agilizar los procesos de gestión y la toma de decisiones, pero, el uso de la tecnología puede crear tantos problemas como los que resuelve. Uno de estos es la seguridad.

El desarrollo y uso masivo de las computadoras y otros medios digitales, ha permitido disponer de otras formas de generar información y se han incrementado las posibilidades de almacenarla, existiendo multitud de dispositivos en los que se puede guardar información de forma digital, siendo llevadas a este formato las informaciones relevantes de la organización.

La información y los recursos del SI, o relacionados con éste, constituyen activos de la organización, necesarios para su funcionamiento correcto y poder alcanzar los objetivos propuestos. Son activos, entre otros, la información y los datos, los recursos físicos (tanto el equipamiento tecnológico como las edificaciones), los recursos humanos (denominados desarrolladores o usuarios, en dependencia de la relación que tengan con el equipamiento) y los recursos de software (tanto los sistemas operativos como las aplicaciones).

Cada activo se caracteriza por el estado de su seguridad, la que se concreta estimando los valores de los atributos confidencialidad, integridad y disponibilidad, es decir, se expanden los atributos de la información y se definen, la confidencialidad como la característica que previene contra la divulgación no autorizada y el acceso físico o lógico; la integridad como la característica que previene contra la modificación o destrucción no autorizadas y la disponibilidad como la característica que previene contra la denegación de acceso no autorizado. Se tiene en cuenta un cuarto atributo, la autenticación, como la característica de dar y reconocer autenticidad, la identidad de los actores y la autorización por parte de los autorizadores (Misfud, 2012), que establece una relación armónica sistema-usuario-aplicación, donde solo se puede acceder a la información y a las aplicaciones a las que se tiene derecho.

1.3 La seguridad de la información y la seguridad informática.

El concepto de seguridad es amplio y abarcador, tomando diversos sentidos según el área o campo de acción de que se hable o al que haga referencia y la percepción que se tenga del activo o elemento que se pretenda que sea seguro. Maslow (1943), ubica la seguridad en el segundo nivel dentro de las necesidades de déficit en la Pirámide de Jerarquía de las Necesidades Humanas y Malinowski (1944), en La Teoría de las Necesidades, entre las siete necesidades básicas a satisfacer por el hombre

Existen varias definiciones de seguridad. Algunas de ellas son:

- Ausencia de peligro, daño o riesgo (Foro de Seguridad, 2014. Recuperado el 27/02/2014 del sitio Web <http://www.forodeseguridad.com>).
- Cualidad de seguro (DRAE, 23^{ra} Edición (2014) Disponible en <http://www.rae.es/diccionario-de-la-lengua-espanola/la-23a-edicio-2014>).
- La ausencia de riesgo o la confianza en algo o alguien (Instituto Superior de Seguros y Gerencia, 2014. Recuperado el 27/02/2014 del sitio Web <http://www.insudeseg.com>)
- La propiedad de algo donde no se registran peligros, daños ni riesgos (Definición de, 2014. Recuperado el 27/02/2014 del sitio Web <http://definicion.de>)

Teniendo en cuenta las definiciones anteriores de seguridad, se puede afirmar que esta no es absoluta, se define respecto a algo o a alguien, por lo que es relativa al sujeto y posee, por tanto, un carácter subjetivo. Es un estado de ánimo, una sensación, una cualidad intangible, un objetivo y un fin que se anhela constantemente como una necesidad primaria.

La condición de seguro es un compromiso entre inseguridad y seguridad. Mientras más se conozcan las inseguridades, mejor preparado se está para enfrentarlas y en esa misma medida se puede afirmar cuán seguro se es. Para entender la seguridad es preciso detenerse en un grupo de conceptos muy relacionados con ella: amenaza, vulnerabilidad, riesgo e impacto.

La amenaza es un evento raro o extremo en el ambiente natural o humano, que afecta adversamente a la vida humana o sus actividades a tal grado de causar daño (Wilches-Chaux, 1989). Es un peligro latente, un evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos (Cupreder, 2000). Al valorar las amenazas podemos conocer qué probabilidad hay de que éstas se lleven a cabo.

Vulnerabilidad es cualidad de vulnerable, es decir, que es susceptible de ser lastimado o herido. Las características de una persona o grupo de ellas en relación con su capacidad de anticipar, enfrentar, resistir y recuperarse de un desastre (Blaikie, 1994). Todo el mundo tiene su propio nivel y tipo de vulnerabilidad, dependiendo de sus circunstancias, lo que hace que sea relativa y que todas las personas y grupos sean, de alguna manera, vulnerables. Algo es vulnerable cuando se encuentra en situación de riesgo.

El riesgo es la posibilidad de que algo malo suceda. Es cualquier fenómeno de origen natural o humano que signifique un cambio en el medio que ocupa determinada comunidad, vulnerable a ese fenómeno (Wilches-Chaux, 1989), la probabilidad de pérdidas futuras, el resultado de la existencia de un peligro latente, que puede producir daños en diversos grados (Cardona, 2007).

El riesgo expresa la probabilidad de materialización de una amenaza, que puede tener éxito debido a una vulnerabilidad. Aunque la probabilidad sea baja, la amenaza puede materializarse, es decir, siempre existe riesgo cuando existe la probabilidad de que ocurra un daño por motivo de que una o más amenazas, se manifiesten en un contexto vulnerable.

El riesgo es un concepto dinámico, pues cambia a lo largo del tiempo y en función de las variaciones producidas en la naturaleza de las amenazas y las vulnerabilidades, por lo que debe ser evaluado periódicamente. Es medible, pudiendo ser determinadas las consecuencias esperadas de materializarse la amenaza, es decir, el impacto que determinados fenómenos tienen sobre la realidad.

El impacto es la impresión o efecto muy intensos dejados en alguien o en algo por cualquier acción o suceso (Moliner, 1988). Se refiere a los cambios en una entidad producidos por una determinada acción. Medir impacto es tratar de determinar lo ocurrido, es establecer causalidad. Las relaciones causales son establecidas en forma probabilística.

Las manifestaciones de estos elementos en la vida, evidencian que es indudable que en el accionar diario se desarrollan actividades e interacciones con el medio, que pueden transformarse en vulnerabilidades que conduzcan a que se materialicen peligros o amenazas, es decir, la vida se desarrolla en un mundo vulnerable, expuesto a riesgos constantes, por lo que toda actividad humana es susceptible a la seguridad, de ahí que existan varios tipos de seguridad: jurídica, laboral, humana, social, pública, tecnológica, informática, entre otras.

El concepto de Seguridad de Informática no debe ser confundido con el de Seguridad la Información. La información adopta variadas formas y es almacenada en diferentes soportes, no solo informáticos. Con frecuencia seguridad informática y seguridad de la información se confunden y pueden parecer lo mismo, sobre todo si se tiene en cuenta que el desarrollo y evolución de las TICs, tiende hacia la gestión de cualquier información, mediante sistemas informáticos. Aunque están destinados a convivir en armonía y trabajar de conjunto, cada una de estas vertientes de la seguridad, tienen objetivos y desarrollan actividades diferentes. Coro Antich (comunicación personal, 20 de junio, 2013) plantea que ambos términos son usados frecuentemente como sinónimos porque persiguen una misma finalidad al proteger la confidencialidad, la integridad y la disponibilidad de la información.

Mientras que la Seguridad de la Información define la línea estratégica de la seguridad, la Seguridad Informática se ocupa de los aspectos tácticos y operacionales. La estrategia de seguridad se manifiesta mediante un Plan Director, abarcador de todos los elementos relacionados con ambos conceptos (*Figura 3*). La Seguridad Informática se apoya en el Plan de Seguridad Informática como herramienta para establecer los principios organizativos y funcionales de la actividad y recoger las políticas de

seguridad y las responsabilidades de cada uno de los participantes en el proceso, así como las medidas y procedimientos para prevenir, detectar y responder a las amenazas.

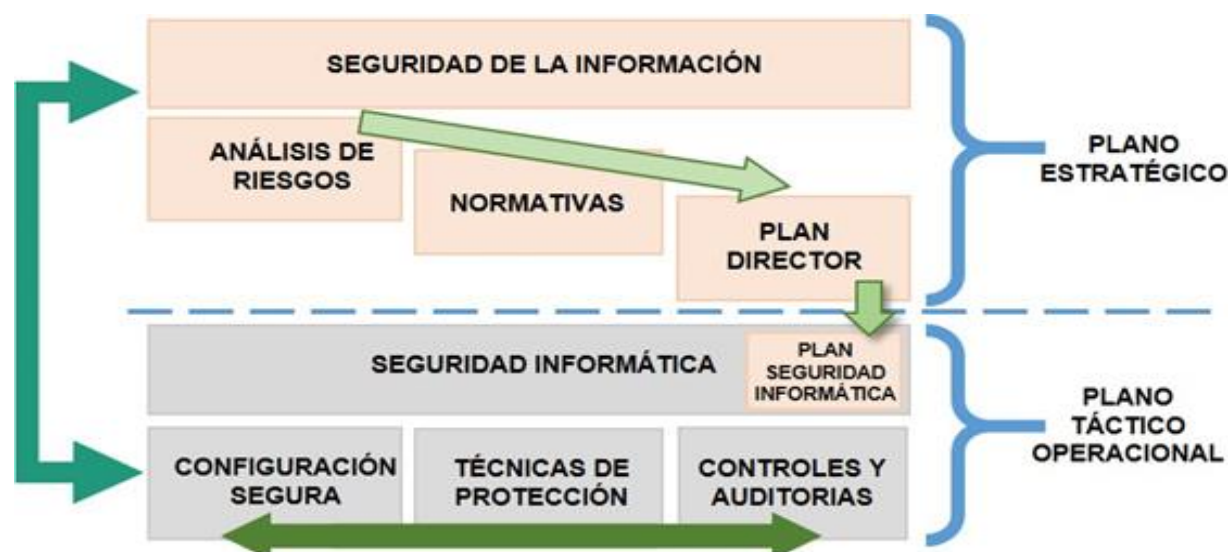


Figura 3. Interacción entre Seguridad de la Información y Seguridad Informática

Fuente: elaboración propia.

En la infraestructura de la empresa, los servicios de TICs son soporte y apoyo a las necesidades de negocio. La estrategia de dirección define objetivos, roles y responsabilidades, además de un proceso de toma de decisiones basado en la información, generalmente sobre un sistema informativo que abarca a todas las áreas de la organización, con un flujo ascendente que le permite a la alta dirección disponer de la información que necesita, de manera rápida, precisa y confiable.

Como expresa Gómez Vieites (2011) en su Enciclopedia de la Seguridad Informática, la información es poder y según las posibilidades estratégicas que ofrece, es un valioso activo de la empresa; sensible a ser conocida solo por las personas autorizadas y crítica al ser indispensable para la operación de la empresa.

Según Ormella (2010), Seguridad de la Información es un concepto más amplio que el de Seguridad Informática, ya que no es simplemente un aspecto técnico, sino que implica la responsabilidad de la alta dirección de la organización y sus cuadros directivos. Es un concepto que tiene en cuenta, no solamente la seguridad tecnológica,

sino también otras facetas de la seguridad, como son, la seguridad desde el punto de vista jurídico, normativo y organizativo. Para Mifsud (2012) es la disciplina que tiene en cuenta los riesgos y las amenazas, analiza escenarios y define las buenas prácticas y los esquemas normativos a asumir. Exige los niveles de aseguramiento de los procesos y las tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

El objetivo de la gestión de la seguridad de la información es asegurar la continuidad de las operaciones de la organización y reducir al mínimo los daños causados por una contingencia, así como, optimizar la inversión en tecnologías de seguridad.

Para el término Seguridad Informática se han dado diferentes definiciones. De ellas, la más abarcadora es la ofrecida por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional (ISO e IEC, por sus siglas en inglés), publicado en octubre de 2005, donde se define que la seguridad informática “consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la disponibilidad, la integridad y la confidencialidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.” (ISO/IEC 27001, 2005).

Teniendo en cuenta lo anterior, es preciso adecuar y complementar los conceptos relacionados con la seguridad en lo relacionado con las tecnologías.

La propia naturaleza de los medios de las TICs, combinación de elementos electrónicos, de transmisión y programas, los hace proclive a fallos, lo que imposibilita que un sistema informático esté libre de todo peligro o riesgo. Esta característica lleva a adecuar la definición de seguridad y se introduce el concepto de fiabilidad, definiéndose esta como la “capacidad de un sistema, o componente, para desempeñar las funciones especificadas, cuando se usa bajo unas condiciones y periodo de tiempo determinados” (ISO 25000, 2005). Por tanto, se habla de sistemas fiables en lugar de sistemas seguros, entendiéndose como tal el que se comporta según se espera, bajo determinadas condiciones en un tiempo dado.

Un sistema informático se dice fiable si los medios técnicos que lo soportan garantizan los tres aspectos básicos de la información: la confidencialidad, la integridad y la disponibilidad (Misfud, 2012). La confidencialidad es la condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados (Anexo a la Resolución 127/07:16), es la protección contra la lectura, escritura o modificación, por personas no autorizadas. La integridad es la garantía de que la información sólo puede ser modificada, incluyendo creación y borrado, por los autorizados; que el sistema no debe modificar o corromper la información que almacene o permitir que alguien no autorizado lo haga (Anexo a la Resolución 127/07:17), ocurriendo de igual forma con los sistemas y programas encargados de dar tratamiento a la misma. Disponibilidad significa la garantía de que los autorizados tengan acceso a la información y activos asociados cuando se requiera; que el sistema se mantiene funcionando y con capacidad de recuperarse en caso de fallo (Anexo a la Resolución 127/07:17).

Por su parte, una amenaza es cualquier acontecimiento que pueda causar daños a los bienes informáticos. Puede ser una persona, un programa maligno o un suceso natural o de otra índole (Anexo a la Resolución 127/07:16). Las amenazas representan los posibles atacantes o factores que inciden de manera negativa sobre las debilidades del sistema.

Las vulnerabilidades son los puntos de los sistemas susceptibles de ser atacados. Representan las debilidades o aspectos falibles o atacables en el sistema informático (Anexo a la Resolución 127/07:18). Es decir, una vulnerabilidad es toda debilidad que comprometa la seguridad de un sistema informático.

El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la organización. (Anexo a la Resolución 127/07:18), siendo el impacto los daños producidos por la materialización de una amenaza (Anexo a la Resolución 127/07:17).

La autenticidad consiste en el método para comprobar o autenticar la identificación de un usuario o proceso. Una vez identificado al usuario, es necesario que este

demuestre, de algún modo, la veracidad de su identidad (Anexo a la Resolución 127/07:16), lo que, generalmente, se realiza mediante la utilización de contraseñas personales.

El no repudio es un método para asegurar que las partes que intervienen en una transacción no nieguen su participación (Anexo a la Resolución 127/07:17). Con esto se evita que el emisor o el receptor nieguen la participación en la transmisión y recepción, respectivamente, de un mensaje.

La ISO, en su Norma ISO 13335: Guías para la gestión de la seguridad de TI, de 1997, define riesgo tecnológico como *“la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o grupo de activos, generándose pérdidas o daños”*. Tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad. Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de las vulnerabilidades y los riesgos a los que se exponen las organizaciones.

La seguridad es relativa, nunca es absoluta, por lo que ningún sistema es totalmente seguro, lo que implica que el riesgo no es totalmente eliminable, ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo y convivir con él, de manera controlada. El riesgo es necesario gestionarlo.

La gestión de riesgo permite determinar, analizar, valorar y clasificar los riesgos, para poder implementar mecanismos acertados que permitan controlarlo. En su forma general contiene cuatro fases:

- **Análisis:** Determina los componentes del sistema que requieren protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el objetivo de determinar su grado de riesgo.

- **Clasificación:** Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción:** Define e implementa las medidas de protección. Sensibiliza y capacita los usuarios conforme a las medidas.
- **Control:** Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las deficiencias y sancionar el incumplimiento.

Para poder enfrentar tantas amenazas de manera coherente, es necesario establecer guías que ilustren cómo abordar la seguridad de una forma responsable, procedimental y orientada al cumplimiento de los estándares mínimos requeridos para la tecnología actual.

Para ello es preciso tener claro el origen de los elementos o factores que amenazan los tres aspectos que caracterizan la información, la confidencialidad, la integridad y la disponibilidad, lo que puede ser analizado desde dos puntos de vistas muy relacionados en su manifestación (*Figura 4*).

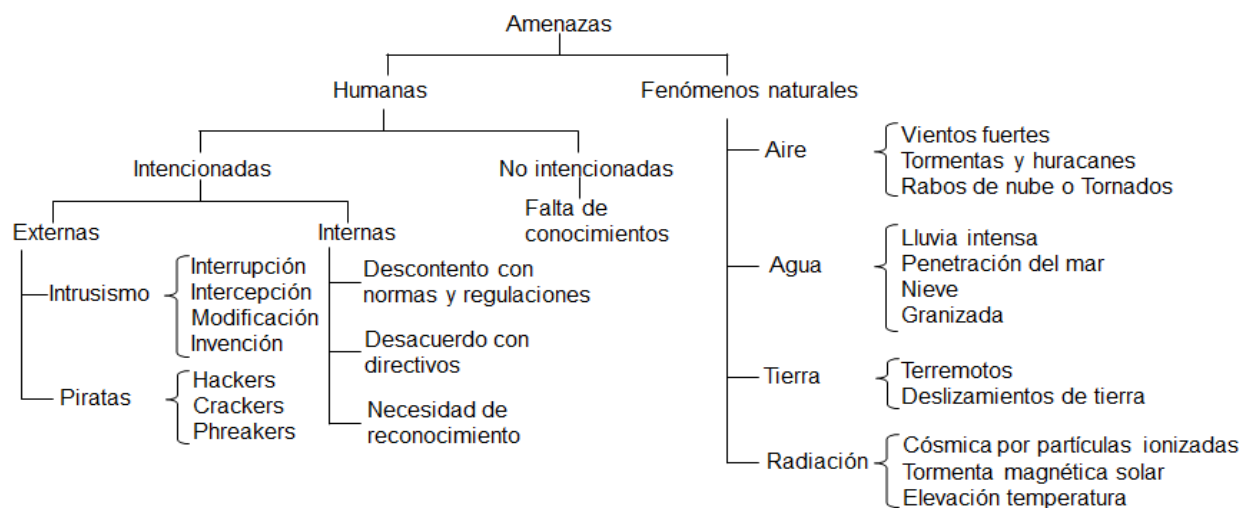


Figura 4 Amenazas a los sistemas por su origen.

Fuente: elaboración propia.

Las amenazas son los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema. Las de origen humano, por su propia naturaleza, son las

más difíciles de detectar y enfrentar, dada la diversidad de manifestaciones posibles: falta de conocimientos, desacuerdo con directivos, descontento con normas y regulaciones, necesidad de reconocimiento, intrusismo con intereses materiales o por satisfacción personal, entre otros. Los fenómenos naturales son impredecibles en su ocurrencia, aunque la no cotidianidad de estos, hace posible establecer, con tiempo, medidas de protección que permitan minimizar daños, incluso pueden simularse y practicar su enfrentamiento.

Existe hoy en el mundo un grupo de entidades con alcance internacional, como ISO, IEC, UIT e IEEE entre otras, que proponen guías, contándose con un elevado número de documentos, considerados normas y asumidos por la mayoría de los estados, buscando estandarizar las soluciones, como una necesidad ante la actual globalización de las comunicaciones y el uso en ascenso de las TICs para compartir información.

La mejor manera de poder implementar esta protección es sobre la base de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información y que se corresponda con el conjunto de bienes informáticos con que cuenta la organización y la importancia y el papel que juegan para el cumplimiento de sus objetivos. Para ello, la organización se vale del Plan de Seguridad Informática.

1.4 El Plan de Seguridad Informática.

Planificar es intentar determinar hoy la realidad que se quiere tener en un momento posterior (Carnota, 1991); es la descomposición de un proceso en pasos claros y articulados y de esta manera, replicados y verificados formalmente (Mintzberg, 1994); es definir los objetivos y determinar los medios para alcanzarlos, analizar por anticipado los problemas, determinar posibles soluciones y señalar los pasos necesarios para llegar eficientemente a los objetivos que la solución elegida define (Mercado, 1996); es una forma concreta de la toma de decisiones que aborda el futuro específico que los gerentes quieren para sus organizaciones, un proceso continuo que refleja los cambios

del ambiente en torno a cada organización y se adapta a ellos (Stoner, 1996); es la primera función administrativa (Chiavenato, 2002).

Las definiciones anteriores permiten afirmar que un plan es un mecanismo organizador, un elemento integrador de soluciones futuras a problemas previsibles, a los que se llega por el estudio y análisis del contexto de lo que se pretende organizar, partiendo de objetivos definidos y sobre la base de los medios utilizables, enmarcando tiempo y responsabilidad.

La Metodología para el Diseño de un Sistema de Seguridad Informática (Dirección de Protección MININT, 2010) contiene un documento complementario, denominado Metodología para la elaboración del Plan de Seguridad Informática, donde se expresa que el Plan de Seguridad Informática (PSI) es la expresión formalmente documentada del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en la organización, recogiendo claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

La Seguridad Informática es preciso verla en dos momentos, distintos pero muy cercanos entre sí, tanto que casi surgen al unísono. Primero el término abarcaba solo la Seguridad de las Tecnologías de la Información, entendiéndose como tal los medios independientes y los involucrados en el proceso de la información de redes locales, el cual fue ampliado posteriormente a Seguridad de las Tecnologías de la Información y las Comunicaciones, una vez que la información comenzó a circular a través de los enlaces establecidos entre estas redes, utilizando diversos medios de enlace.

La **Figura 5** muestra el ámbito de acción del PSI, como documento en el que se refleja el conjunto de medidas técnicas y organizativas a ejecutar, en su relación con la seguridad de la información y seguridad informática.

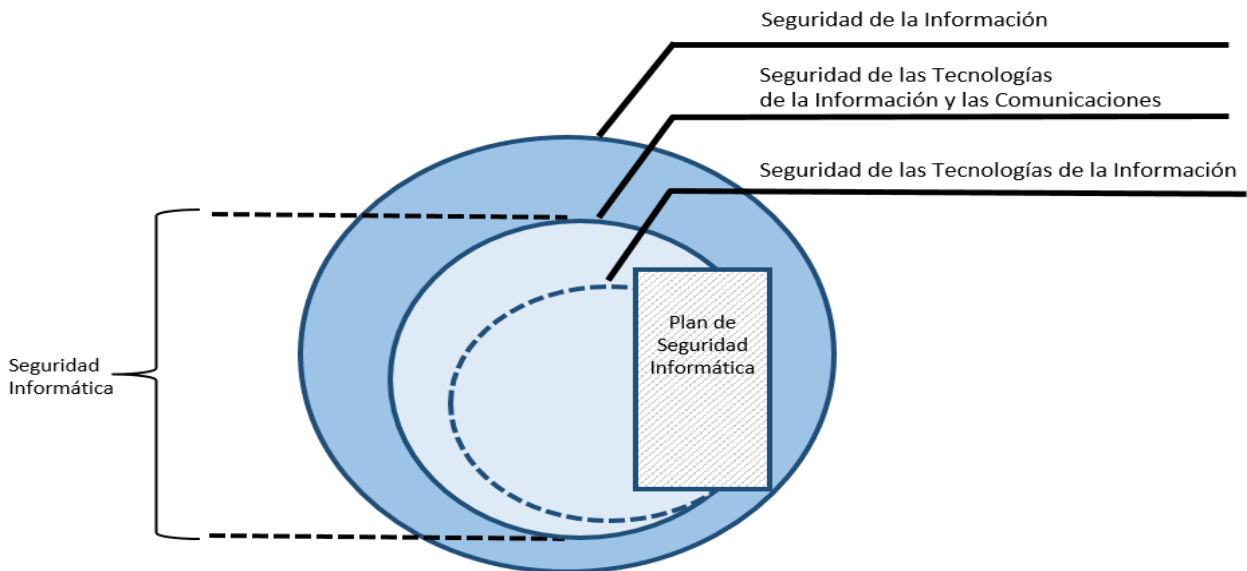


Figura 5. Ámbito de acción del PSI.

Fuente: elaboración propia

El PSI se enfoca en la protección de la infraestructura de TICs del sistema y todo lo relacionado con la información que por ella se mueve y en brindar los mecanismos para hacer que los riesgos sean minimizados, así como las formas de recuperarse de algún daño que pueda ser sufrido. Es una herramienta de planificación para organizar el enfrentamiento de amenazas y la disminución de riesgos, actuando sobre el ambiente de control de la organización y contribuyendo a la coherencia y fortalecimiento del Sistema de Control Interno.

El despliegue físico de la entidad y el sistema informativo asumido para su gestión, determinan la definición del Sistema de Seguridad Informática, que va a condicionar los niveles de estructuración del PSI, por lo se definen su estructura y contenido, basados en aspectos que deben estar bien enunciados y ser de conocimiento de todos los que se relacionan con las TICs. De forma general, en Cuba se declaran en el PSI, según la Metodología para la Gestión de la Seguridad Informática de la OSRI²:

1. Alcance del PSI
2. Caracterización del Sistema Informático
3. Resultados del Análisis de Riesgos

² OSRI: Oficina para la Seguridad de las Redes Informáticas.

4. Políticas de Seguridad Informática
5. Responsabilidades
6. Medidas y Procedimientos de Seguridad Informática
 - a. Clasificación y Control de los Bienes informáticos
 - b. Del Personal
 - c. Seguridad Física y Ambiental
 - d. Seguridad de Operaciones
 - e. Identificación, Autenticación y Control de Acceso
 - f. Seguridad ante Programas Malignos
 - g. Respaldo de la información
 - h. Seguridad en Redes
 - i. Gestión de Incidentes de Seguridad
7. Anexos del Plan de Seguridad informática
 - a. Listado nominal de usuarios
 - b. Registros
 - c. Control de Cambios

El análisis de riesgo se basa en la norma ISO/IEC 27005:2008 y se enfoca en:

- la clasificación de la importancia de los bienes informáticos,
- las vulnerabilidades del sistema implantado para las TICs,
- las amenazas a los bienes aprovechando las vulnerabilidades,
- la probabilidad (riesgo) de materialización de esas amenazas.

Las Políticas de Seguridad Informática, hacen referencia a la forma de comunicación con los miembros de la organización, al establecer normas de actuación en relación con los recursos y servicios informáticos de la organización. Una política de seguridad informática no es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas, es una descripción de lo que se debe proteger y debe llevar a una posición consciente y vigilante del uso de las TICs.

Las Responsabilidades dejan bien definidos los involucrados en cada parte del sistema y el compromiso que asume con el mismo. La aprobación final del PSI involucra a los

máximos responsables, por nivel de compromiso y participación, garantizando así que cada área con responsabilidad directa en la confección del plan certifique la conformidad con lo expresado.

1.5 Normatividad para la Gestión de la Seguridad Informática.

En el ámbito de las TICs no se ha conseguido definir un modelo universal de toda su actividad que contemple, desde la más detallada tarea técnica, hasta la definición, al más alto nivel, de la estrategia alineada con el negocio.

El interés por mejorar las actividades de las TICs ha hecho que se hayan ido desarrollando varios marcos o modelos que cubren las principales aristas de la gestión de TICs. A veces son complementarios entre sí, en otros aspectos se solapan y, con frecuencia, presentan enfoques distintos sin ofrecer una integración clara con otros modelos o aproximaciones. A pesar de ello, es útil trabajar con estos modelos de referencia ya definidos, por los beneficios que aportan a las organizaciones, como base para avanzar. En la *Figura 6* se muestra un esquema que permite realizar una primera aproximación a este mundo de normas, modelos y marcos de referencia, realizada por la consultora Gartner Group³.

En ella, se ubican las normas en función de dos conceptos, el ámbito de aplicación y el tipo de uso de la normativa. El ámbito de aplicación de las normas ocupa las columnas de la tabla y se divide en el alcance general de la empresa y el alcance de disciplinas específicas de TICs. El tipo de uso de la normativa se representa en tres filas, correspondiendo la segunda fila a las directrices y mejores prácticas. Se aprecia la concentración de propuestas de directrices relativas a las funciones de TICs.

De todas las normas establecidas, llaman la atención la serie ISO/IEC 27000 (*Anexo 1*) para la gestión de TICs, que incluye normas de requisitos para un sistema de gestión de la seguridad de la información, gestión de riesgos, medición y métricas y directrices de implementación. Todas vieron la luz a partir del 2005 y han sido actualizadas

³ **Gartner Group Inc.:** empresa líder mundial en consultoría e investigación de las tecnologías de la información. Tiene su sede en Stamford, Connecticut, Estados Unidos.

durante todos estos años, siendo las últimas actualizaciones de 2013 para la ISO/IEC 27001.

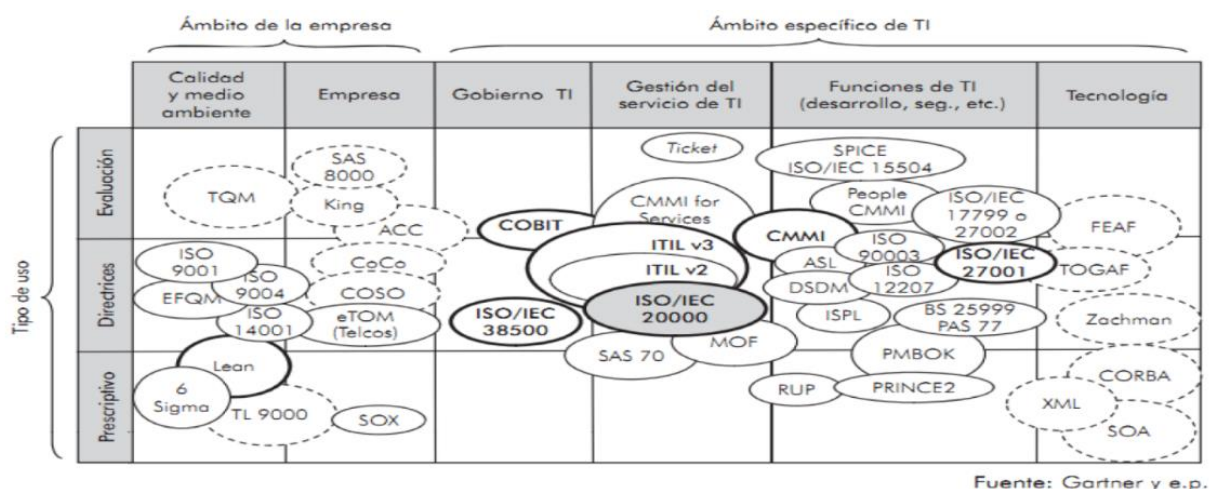


Figura 6. Mapa de las diferentes normas y marcos de referencia relacionadas con las TI.

Fuente: Gartner Group

Como quiera que estas normas se precisan para un mejor entendimiento global y garantizar compatibilidad, a la vez que responden a principios de calidad, se han establecido un grupo de entidades certificadoras, reconocidas mundialmente y que constituyen instrumento para verificar la correcta implantación de las normas y su cumplimiento por las empresas, tanto a nivel nacional como internacional.

Actualmente las legislaciones nacionales de los estados obligan a las empresas e instituciones públicas a implantar políticas de seguridad, por lo que estas normas son asumidas por la mayoría de los países, realizando cada uno adecuaciones en correspondencia con su legislación, estandarizando así la forma de gestionar los riesgos, permitiendo a su vez la compatibilidad de aplicaciones y servicios y su uso seguro.

En Cuba, a partir de la llegada de Internet, y a pesar de lo reducido de su presencia en el ámbito nacional, se tomaron medidas de índole legal para ordenar y regular su uso, así como los medios de trabajo que se utilizan, enfocado principalmente a las computadoras personales de trabajo. La mayoría de estas legislaciones, dan

tratamiento al tema de la seguridad informática en las empresas, así como de los medios físicos en que se elabora información.

El modelo de gestión de la seguridad que se asume en Cuba es el que propone la Norma ISO/IEC 17799:2000 (*Figura 7*), establecido por la OSRI en su Metodología para la Gestión de la Seguridad Informática.

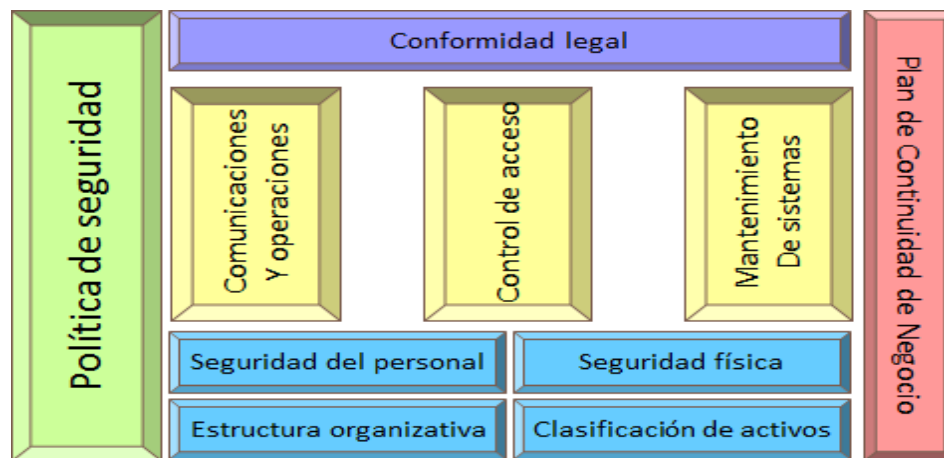


Figura 7. Modelo de gestión de la seguridad

Fuente: ISO/IEC 17799:2000

Esta Norma adopta el modelo "Planificar - Hacer - Verificar - Actuar" (PHVA) para estructurar todos los procesos del SGSI. La *Figura 8* ilustra cómo un SGSI toma como entrada los requisitos y expectativas de seguridad de la información de las partes interesadas y, a través de las acciones y procesos necesarios, produce los resultados de seguridad de la información que cumplen esos requisitos y expectativas.

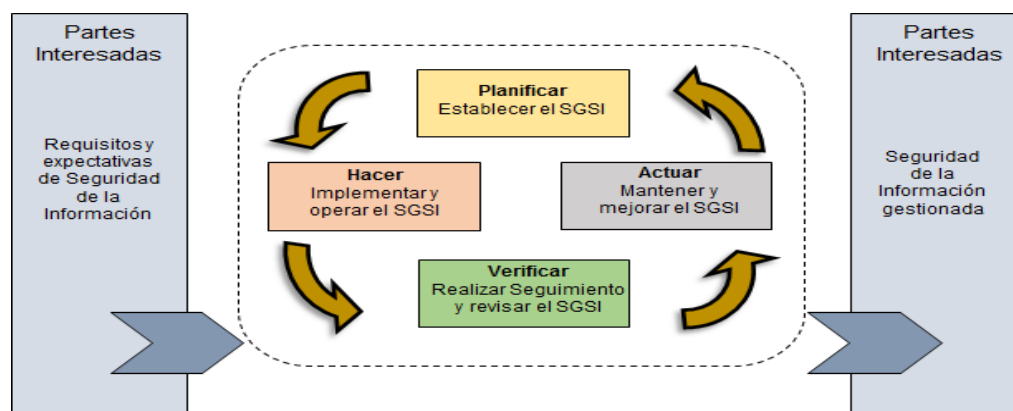


Figura 8. Modelo de PHVA aplicado a los procesos del SGSI

Fuente: ISO/IEC 17799:2000

En el *Anexo 2* se exponen las legislaciones más significativas que se han dictado en Cuba desde que se inició el uso masivo de las TICs en las organizaciones cubanas.

En lo concerniente a la seguridad informática, el Decreto Ley 199 presenta las siguientes deficiencias:

- Se limita la importancia de las TICs a que las mismas procesen, conserven, intercambien o reproduzcan información confidencial, dando competencia al MININT⁴ y al SIME⁵ para regular estos procesos, obviándose informaciones con otras clasificaciones, de gran importancia también para las organizaciones y su gestión.
- Delega en el MININT la facultad de realizar y autorizar la realización de las auditorías de Seguridad Informática, existiendo en la actualidad dualidad de funciones con la Contraloría General de la República.
- Carece de apartado que implique sanciones o demás acciones coercitivas.
- Cuenta con un grupo de disposiciones complementarias dirigidas a la elaboración de Planes de Seguridad Informática y Contingencias, proponiendo una estructura esquemática de los planes y adecuando a las necesidades particulares solo ciertos aspectos de la actividad, lo que provoca que, en muchos casos, estos Planes revistan carácter clasificado y no son del conocimiento de los usuarios, lo que los limita de conocer la conducta a adoptar ante la ocurrencia de hechos que atenten contra la seguridad informática.

La estrategia de informatización de la sociedad en Cuba y los avances alcanzados en los últimos años en este particular en todos los sectores, a partir del incremento de tecnologías de la información y sus servicios asociados, así como las orientaciones dadas por la dirección del país, encaminadas al desarrollo de programas que consoliden y multipliquen lo logrado, llevan a las organizaciones a adoptar medidas que garanticen adecuados niveles de seguridad.

⁴ **MININT:** Ministerio del Interior.

⁵ **SIME:** Ministerio de la Sidero Mecánica y la Electrónica. Hoy las funciones relacionadas con la informática y las comunicaciones las ejerce el Ministerio de Comunicaciones.

Capítulo II. Planificación de la seguridad informática en Cubana de Aviación S.A.

2.1 Evolución de la empresa Cubana de Aviación S.A.

En octubre de 1919 es fundada en La Habana, por el rico negociante azucarero Aníbal Justo de Mesa, una de las más antiguas líneas aéreas conocidas en América Latina, la Compañía Aérea Cubana. Un año después, en octubre de 1920, se inicia la primera ruta de aviación civil comercial que operara en Cuba, con capital íntegro cubano. El año que medió entre una fecha y otra, se ocupó en la adquisición de las aeronaves, las solicitudes de asistencia técnica y de vuelo y popularizar la aviación en el país al establecerse una escuela y organizar paseos aéreos alrededor de la ciudad de La Habana, para eliminar la desconfianza acerca del peligro de volar.

En enero de 1922 se disuelve la Compañía ante la pérdida del auge del servicio comercial, como consecuencia de los estragos de la Primera Guerra Mundial. Se establecen así, por otras compañías, líneas regulares entre Cayo Hueso y La Habana, empleando hidroaviones, destacándose la Compañía Cubana Americana de Aviación y la Florida West Indies Airways. Esta última se fusiona con la constructora de hidroaviones Aeromarine y forman la Aeromarine West Indies Airways Incorporated, quedando inaugurada, el 1ro de noviembre de 1920, la primera ruta postal aérea entre La Habana y Cayo Hueso.

En el mes de junio de 1921 fue suspendido este servicio y el 19 de octubre de 1927, resurge bajo la compañía Pan American Airways Incorporated, que el 1ro de febrero de 1929 inaugura oficialmente y con carácter provisional, el servicio aéreo doméstico de pasajeros entre La Habana y Santiago de Cuba, con escala en Camagüey.

En 1928 surge la Corporación Aeronáutica de Cuba, S.A., que llega a ser la primera transportadora de correspondencia y pasaje, entre enero y marzo de 1931, entre diferentes puntos de la nación. También en 1928 opera entre Miami y La Habana la Cuban American Airlines y en febrero de 1929, Servicio Cubano de Aviación, S.A. establece una ruta aérea nacional de mercancías y pasajeros.

Marrón Duque de Estrada (2010) resume el comienzo definitivo de una aerolínea cubana cuando expresa:

El 8 de octubre de 1929, la North American Aviation, a través de su subsidiaria Intercontinental Aviation, estableció la Compañía Nacional Cubana de Aviación Curtiss, S.A., una empresa de un millón de pesos a cuya organización favorecieron muchas figuras prominentes de la política, la banca y el mundo de los negocios, capital norteamericano y la ayuda del Gobierno cubano con un subsidio mensual de \$10 000 para el transporte del correo aéreo nacional, la que casi de inmediato inauguró un servicio aéreo doméstico el 4 de julio de 1930, de La Habana a Santiago de Cuba, con escalas intermedias, hasta convertirse más tarde en factor determinante del progreso y desarrollo económico y social de nuestro país, que contribuyó, además, a estrechar las relaciones con todos los pueblos del mundo. (p.10).

Durante 30 años, la Compañía Nacional Cubana de Aviación Curtiss, S.A fue la encargada del transporte de pasajeros, carga y correo en el territorio nacional, a la vez que expandía su presencia por el mundo, estableciendo gerencias en diferentes países y garantizaba el enlace con el resto del mundo. Durante este tiempo surgieron otras compañías para la gestión aeroportuaria que acompañaban a Cubana de Aviación en las actividades relacionadas con la aviación. El 27 de junio de 1961, el Ministro encargado de la Corporación Nacional de Transporte dictó la Resolución AEE-86, creando, con personalidad propia la Empresa Consolidada Cubana de Aviación, que agrupaba las funciones de todas las empresas dedicadas a la actividad del transporte aéreo en el país y en el exterior.

En 1993 se crea la Corporación de la Aviación Civil S.A. (CACSA), conformada por las empresas que resultaron de la división de la Empresa Consolidada Cubana de Aviación, para atender diferentes funciones relacionadas con la actividad de transporte aéreo, tanto de pasajeros como de carga, surgiendo, entre ellas, Cubana de Aviación S.A. (CU), dedicada al transporte de pasajeros, carga y correo, con representación en más de 30 países.

Desde la introducción de tecnologías informáticas en Cuba, CU ha sido poseedora de medios de este tipo, dedicándolos fundamentalmente al registro de estadísticas y a la contabilidad. De igual forma comenzó a utilizar estas tecnologías para el control de reservas y otras funciones de la aviación, desde el surgimiento de los primeros sistemas automatizados para estos fines. Desde ese momento, en CU se ha tenido un sistema de seguridad informática, que ha ido evolucionando en la misma medida en que lo ha hecho la tecnología y la información que en ella se soporta.

La empresa ha vivido diversos cambios y ajustes a lo largo de estos años, estando, en la actualidad, organizada de manera jerárquica en dos niveles bien definidos, uno donde se agrupan las áreas de regulación y control, constituido por Direcciones, Departamentos independientes y Grupos y el otro que agrupa a 4 Unidades Empresariales de Base (UEB), encargadas de ejecutar las actividades generadoras de recursos y la logística de la empresa. Dentro de las Direcciones de las áreas de regulación y control está definida una Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), que tiene como función principal establecer las metodologías y procedimientos generales de trabajo, tanto para las propias áreas de regulación y control, como para las UEB, así como el seguimiento y control de los mismos.

La DTIC define, para toda la empresa, los Sistemas Operativos a implementar, tanto de red como en las estaciones de trabajo; el equipamiento a utilizar, garantizando la uniformidad del hardware, las aplicaciones y sistemas generales a explotar y las políticas de seguridad a seguir, como el Sistema Antivirus y las reglas para contraseñas, para evitar incidentes y accidentes informáticos.

De igual forma, determina las características de los puestos de trabajo en cuanto a las tecnologías necesarias para el cumplimiento de funciones y los conocimientos y habilidades (competencias digitales) que deben poseer los usuarios de las tecnologías para el desarrollo de su trabajo.

Todo esto se ejecuta en correspondencia con las indicaciones que se reciben del ente superior, la CACSA, que cuenta con una Dirección de Tecnologías de la Información y las Comunicaciones (DTIC-CACSA), encargada de dirigir, metodológicamente, el

trabajo de las TICs en todas las empresas que componen la Corporación. Esta Dirección tiene una función metodológica y de control y, partiendo de la legislación vigente en Cuba al respecto y de normas internacionales, elabora la documentación referente a la seguridad de las TICs que debe ser tenida en cuenta por cada entidad para elaborar las estrategias a seguir. Se define que los máximos responsables de la seguridad de la información, a cada nivel, son los directivos.

CU, como parte integrante de la CACSA, organiza el trabajo de esta esfera partiendo de las indicaciones de DTIC-CACSA, adecuando a su entorno la legislación vigente en el país y tomando en cuenta las tendencias nacionales e internacionales, para lograr una gestión adecuada de sus tecnologías, con una protección elevada de la información.

El seguimiento y control de la actividad se expone anualmente en un informe al Consejo de Dirección de la empresa, en el que se presentan los resultados obtenidos en el año y las principales deficiencias presentadas. Trimestralmente se realiza el análisis de la navegación por Internet, el uso del correo electrónico y otros servicios y el análisis de incidentes y sus correspondientes medidas administrativas. Se realizan en el año dos reuniones de trabajo con Jefes de Unidades nacionales e internacionales, momentos en los que se analiza con estos todo lo relacionado con las TICs y sus usos.

Para realizar el estudio que se presenta en este informe, se tomó como base la información recogida en los documentos resultado de las acciones antes mencionadas, los análisis de riesgos y los PSI elaborados en los últimos 5 años. También fueron objeto de análisis el Flujo Informativo definido en la empresa, el Decreto Ley 199/99 Sobre la Seguridad y Protección de la Información Oficial, la Resolución 6/1996 que pone en vigor el Reglamento sobre la Seguridad informática y la Resolución 127/2007, Reglamento de Seguridad de las Tecnologías de Informática y Comunicaciones.

Se sostuvieron encuentros sistemáticos de trabajo con el Jefe de Departamento de Control Interno, el Director de Protección y Seguridad y la Jefa de la OCIC, así como reuniones de trabajo con diferentes directivos, entre ellos los Directores Comercial, Económico, de Operaciones y de la Técnica y se realizaron entrevistas a directivos,

especialistas y técnicos usuarios de las TICs, en las que se abordaron temas relacionados con la responsabilidad ante la información y su seguridad, el conocimiento de las normas y regulaciones sobre seguridad informática y el uso de las TICs.

En el marco de la DTIC se asignaron las áreas de la empresa a los diferentes especialistas relacionados con el tema, incluyendo las unidades nacionales y en el exterior, las que fueron visitadas y donde se realizaron los análisis de riesgos correspondientes. Para el estudio presentado se consideró lo realizado en los últimos 4 años, sosteniéndose reuniones de grupo para el estudio y análisis de la información obtenida, lo que permitió elaborar procedimientos de trabajo que fueron aplicados en cada momento y ampliados al uso en toda la empresa.

2.2 Caracterización del Sistema Informático.

CU, para garantizar su misión empresarial, presenta dos singularidades: su dispersión geográfica (*Anexo 3*) y la gran diversidad de procesos (*Anexo 4*). Estas singularidades condicionan el sistema de TICs de la entidad, implicando el empleo de redes de diferente tipo en cuanto a su ámbito de operación y un considerable número de sistemas y aplicaciones diferentes.

La matriz DAFO de las TICs, realizada por la DTIC para determinar los aspectos que inciden, tanto positiva como negativamente, en el uso de las mismas, arroja una serie de debilidades y amenazas que inciden directamente en la gestión de la seguridad de las TICs, lo que implica la necesidad de realizar un análisis de riesgos amplio y profundo.

La entidad tiene presencia en casi la totalidad del territorio nacional, ya sean Unidades de Ventas o Puntos de ventas asociados a estas y representación en 20 países. En una misma zona, como el Aeropuerto Internacional José Martí, en La Habana (HAV-AIJM), el grado de dispersión geográfica es grande al no disponer de una edificación única para todas las dependencias, motivado por las funciones y obligaciones de los diferentes grupos de trabajo, los que necesitan estar lo más cerca posible del lugar donde ejecutan dichas funciones.

Esta dispersión caracteriza el SI, provocando, a su vez, dispersión en las TICs que le da soporte y dificultando el servicio y la atención a las mismas. En torno al SI se manifiestan deficiencias, evidenciadas durante el análisis que se realizó en la empresa referente a la información clasificada, según lo establece el Decreto Ley 199, detectándose falta de conocimientos y responsabilidad. Entre las fundamentales se encuentran:

- Los generadores de información no la clasifican de manera correcta.
- Duplicidad en la información que viaja vertical al solicitarse informaciones similares por diferentes áreas metodológicas, lo que significa la presencia de brechas en la comunicación horizontal entre las áreas.
- Informaciones solicitadas por la CACSA anualmente que no ha sido modelada y presenta omisiones.
- Áreas que no tienen definido su SI o presentan deficiencias, provocando que la información no fluya correctamente o en tiempo.
- El área rectora del análisis y perfeccionamiento del SI no ejerce la influencia necesaria para que este proceso sea correcto.

Todo esto genera una alta cantidad de amenazas al sistema informático desplegado y a la información que por él se mueve y se almacena, existiendo, igualmente, un alto número de riesgos posibles de manifestarse, ante las vulnerabilidades manifiestas en el sistema informático.

Las características de la ubicación física donde se encuentra localizada una entidad, influyen directamente en las condiciones de seguridad, por lo que es preciso realizar análisis de riesgos acorde a estas ubicaciones. Cuando más de una entidad comparte el espacio físico, comparte también sus riesgos, compartiendo los directivos de cada una, la responsabilidad de atención al sistema de seguridad.

Por otra parte, existe poca conciencia en los directivos, lo que se manifiesta en las intenciones de traspasar a DTIC todo lo relacionado con la información y los medios informáticos, evidenciándose en los análisis conjuntos que al respecto se efectúan y las propuestas de responsabilidad en las medidas de enfrentamiento.

El flujo de la información está diseñado en función de las necesidades de la organización y de los que hacen uso de la misma. Tanto los datos como las aplicaciones utilizadas para su gestión, ya sean las desarrolladas en la propia empresa, como las adquirida a terceros, responden a las necesidades y expectativas requeridas para el cumplimiento de los objetivos de la entidad.

Al ser una empresa compleja, el cumplimiento de su misión conlleva la gestión de múltiples procesos, siendo los fundamentales, en orden de importancia: Comercial, Operacional, Servicios Técnicos a las aeronaves y Contabilización de Boletos. Cada uno está compuesto por varios subprocesos, que abarcan todas las áreas de la empresa y que se ejecutan independientes, pudiendo ocurrir en paralelo, garantizando la interrelación entre cada uno de los procesos.

Las fuentes de información son diversas, fluyendo hacia y desde las entidades en el exterior, las unidades nacionales, las áreas vinculadas directamente con la actividad fundamental, la CACSA y de entidades internacionales de imprescindible participación en la aviación civil. Es importante hacer notar que las unidades de venta de la empresa, tanto nacionales como en el exterior, cuentan con oficinas auxiliares en los aeropuertos donde opera la aerolínea y en otras ciudades, que constituyen puntos de incidencia de la información,

Una gran cantidad de información es intercambiada de manera digital, a través de sistemas y aplicaciones informáticas, como la referente a las reservas y los pasajeros volados, informaciones sobre condiciones meteorológicas, planes de vuelo, transacciones comerciales, etc., mientras que para otras existen modelos para su captación y que son introducidas al sistema mediante software de uso contable, de ventas, conformación de bitácoras de vuelo, etc.

Las legislaciones y demás documentos rectores que rigen los aspectos de la seguridad de la información y la seguridad informática en los países donde CU posee representación, están, al igual que las vigentes en Cuba, basadas en las normas internacionales, lo que garantiza la compatibilidad en los análisis y las medidas que se desprenden para organizar el trabajo de las TICs y enfrentar las deficiencias que se

presenten. También es una práctica generalizada a nivel mundial y presente en estos países, la existencia de Códigos de Ética y Reglamentos para el uso de las TICs, basado en estándares internacionales.

En el aspecto Comercial hay tres servicios sumamente importantes, dos relacionados con los pasajeros: la gestión de la venta de boletos y la gestión para la publicación de las tarifas y el otro vinculado con las guías aéreas necesarias para el transporte de carga. Para garantizar los dos primeros se requiere la conexión a sitios de hospedaje de esos servicios, uno de ellos en las instalaciones de Iberia en Madrid y de ahí hacia el proveedor internacional Amadeus, con igual ubicación geográfica, para la gestión de ventas. Para la gestión de las tarifas se requiere también de Amadeus y otro sitio denominado ATPCO, hospedado en EE.UU.

Para la gestión de los servicios de carga se requiere la conexión al sitio de hospedaje de este servicio, también en las instalaciones de Iberia en Madrid. La página WEB de la empresa, para la gestión de ventas por Internet, se encuentra hospedada en Canadá y puede ser consultada desde cualquier lugar del mundo, pudiéndose realizar reservas y los pagos correspondientes, mediante las tarjetas de créditos que no son vetadas por las leyes del bloque de los EE.UU.

En el aspecto operacional, se requiere cumplir con las regulaciones establecidas por IATA⁶ y su división de Seguridad Operacional IOSA⁷, lo que requiere el control de la utilización de la flota de aeronaves, las tripulaciones y la emisión de los planes de vuelo antes del despegue. En esta dirección se utilizan aplicaciones para el Control de Flotas y mensajería operacional tipo B, conocida como SITATEX, soportadas por la red de SITA⁸ y garantizada su conexión internacional a través de un centro de datos ubicado en Londres.

⁶ **IATA:** Asociación Internacional de Transporte Aéreo (*International Air Transport Association*)

⁷ **IOSA:** Auditoría de la Seguridad Operacional de la IATA (*IATA Operational Safety Audit*)

⁸ **SITA:** Sociedad Internacional de Telecomunicaciones Aeronáuticas. Posee una red de alcance global para dar soporte a los servicios aeronáuticos. Entre los servicios que brinda se encuentra el sistema de mensajería conocido como SITATEX, para el intercambio de información operacional en formato texto. Se utiliza en diferentes procesos relacionados con las actividades aeroportuaria y aeronáutica.

Mezclándose los aspectos anteriores, aparece la Información Adelantada de Pasajeros (API) y de Tripulantes (API CREW) y la Información Adelantada de Carga (ACI), que requiere su envío garantizado hacia países donde se encuentra el destino del viaje de la aeronave o hacia países que deben ser sobrevolados al estar en la ruta de vuelo, relacionados con regulaciones asociadas a la seguridad de dichos territorios, como son los casos de EE.UU. y Canadá.

En los Servicios Técnicos a las aeronaves, se encuentra el registro de su funcionamiento, de importancia para los constructores de las mismas, el control de los agregados empleados, sus horas de uso y su tiempo de vida entre otros. Para ello se emplean sistemas para la comunicación cifrada hacia territorio ruso, a través de un enlace directo con Moscú.

La contabilidad de la venta de boletos y guías aéreas, conocida como Contabilidad de Ingresos o *Revenue Accounting*, permite controlar las ganancias de las ventas y dirimir los adeudos y ganancias con otras aerolíneas con la que se tienen acuerdos comerciales⁹, a través de la división de IATA denominada *Clearing House*¹⁰. Otras funciones transaccionales bancarias se ejecutan por la entidad económica internacional BSP¹¹, mediante un fuerte e interesante mecanismo soportado en la infraestructura informática de redes de Internet.

El control de los aspectos contables de la entidad, diferentes al de la boletería, se realiza actualmente por una aplicación propia desarrollada sobre una minicomputadora de procedencia norteamericana, AS-400. Esta aplicación, a pesar de ser un desarrollo propio, no se encuentra certificada y está siendo sustituida por el Sistema Integrado de Gestión eTES¹², de la empresa DATYS¹³, que es empleado en todo el sistema de

⁹ **Acuerdos comerciales:** Códigos compartidos (CS), Acuerdos interlineales para el uso de ticket electrónico (IET), *Acuerdos interlineales para check in (IATCI)*.

¹⁰ **IATA Clearing House:** Cámara de Compensación de la IATA. Es la caja de compensaciones de la IATA para pagos interlineales.

¹¹ **BSP:** *Billing and Settlement Plan*. Plan de Facturación y Liquidación, implantado por las compañías aéreas, a través de la IATA, para la liquidación de los billetes emitidos por las agencias de viajes.

¹² **eTES:** *electronic Total Enterprise Solution*. Solución modular, integrada y adaptable para el manejo de los procesos de compras, ventas, producción, inventario, administración de recursos humanos, emisión de nóminas, control de activos fijos y contabilidad de las empresas. Responde al concepto de ERP (*Enterprise Resource Planning* o Planificación de Recursos Empresariales).

¹³ **DATYS:** Empresa cubana productora de bienes y servicios informáticos.

empresas de CACSA para centralizar los datos contables. Actualmente en CU se trabaja en el despliegue operacional de dicha aplicación.

Es usual en las áreas con participación en los aspectos operacional y técnico, la tendencia a adquirir aplicaciones sin un análisis previo del cumplimiento de los requisitos de seguridad exigidos por todas las instancias, centrándose únicamente en la obtención de la funcionalidad requerida, lo que pone en riesgo la estabilidad del sistema informático y la compatibilidad con la tecnología instalada y el resto de las aplicaciones.

Para el resto de las gestiones de la entidad se emplean dos herramientas de comunicación: la Mensajería Instantánea (IM) y el Correo Electrónico (utilizando la aplicación MDaemon), ésta última en más del 95% de las gestiones efectuadas y constituyendo el medio principal de diseminación de datos e información entre las diferentes áreas de la empresa, incluyendo las unidades nacionales y en el exterior.

El uso del correo electrónico como principal herramienta para el trasiego de información, hace vulnerable al sistema informático en varios aspectos. Es usual el intercambio, entre directivos o entre directivos y especialistas, de información con algún nivel de clasificación, poniéndola en riesgo al poder ser consultada, desviada, modificada o eliminada por algún usuario con permisos y privilegios mal asignados y con intenciones de dañar la misma, ya sea por beneficio personal o para causar otros problemas.

También es usual la congestión de líneas de comunicación y tramos de red, los espacios de almacenamiento en los discos de los servidores y los buzones personales de los usuarios, por el uso indiscriminado de la mensajería, acompañada de ficheros de gran tamaño, en ocasiones ajenos a temas laborales.

La función de la red es compartir información y recursos a distancia, procurando que dicha información sea segura, esté siempre disponible y que sea accesible de forma rápida, siendo indispensable garantizar la fiabilidad del sistema desde los aspectos físicos y lógicos, teniendo que lograr adecuadas condiciones ambientales de

temperatura y humedad, restringiendo el acceso a áreas y locales tecnológicos y manteniendo una compartimentación estricta de permisos y privilegios sobre los medios y la información.

La red de CU se considera una subred de la denominada AVIANET, perteneciente a la CACSA. La licencia jurídica de operación de la primera está determinada por la licencia de operación de la segunda. Desde el punto de vista tecnológico, por su alcance geográfico, la red de CU es de tipo WAN¹⁴, conteniendo, a su vez, subredes de tipo MAN¹⁵ (zona aeroportuaria de La Habana) y redes LAN¹⁶ (unidades de ventas nacionales y en el exterior).

Desde la óptica del espacio de direcciones IP¹⁷ disponibles, es una red clase B¹⁸, estando la misma segmentada, estableciéndose reglas para los tráficos entre los segmentos que la componen. Esta configuración interna es lograda mediante el empleo de equipamiento activo (*switches* y *routers*) capa 2 (L2) y capa 3 (L3) para la segmentación de la red en tramos, a través de segmentos de redes virtuales¹⁹ y las correspondientes listas de control de acceso. Esto permite, unido al uso de contraseñas y la especificación de permisos de acceso y diferentes niveles de privilegios para el uso de la información, lograr la autenticación de los que hacen uso de la misma y poder conocer de la participación en las transacciones entre dos o más partes.

Cuando son violadas las normas para la conformación de contraseñas fuertes y su uso personal, se abren brechas en el sistema de seguridad al ser, por un lado, fáciles de detectar y, por otro, no existir correspondencia entre el dueño de la contraseña y quien

¹⁴ **Red de área amplia (WAN):** red de comunicaciones de datos que abarca un área geográfica relativamente amplia y que utiliza los servicios de transmisión proporcionados por proveedores comunes, como compañías de teléfono.

¹⁵ **Red de área metropolitana (MAN):** red de comunicaciones de datos que abarca zonas extensas de cobertura, dentro de una ciudad o municipio.

¹⁶ **Red de área local (LAN):** red que se limita a un área relativamente pequeña tal como un cuarto, un solo edificio, una nave o un avión.

¹⁷ **Dirección IP:** etiqueta numérica que identifica, de manera lógica y jerárquica, un dispositivo (PC, impresora, *router*, *switch*, módem) que posee una interfaz de red o elemento de comunicación/conexión (tarjeta de red,) y que utilice el protocolo IP (*Internet Protocol*),

¹⁸ **Red Clase B:** red de tamaño mediano por la cantidad de direcciones IP que maneja. Puede tener hasta 65,534 direcciones IP (equipos conectados).

¹⁹ **Red virtual o VLAN:** tipo de red LAN lógica, montada sobre una red física, con el fin de incrementar la seguridad y el rendimiento.

la está utilizando en un momento dado, imposibilitándose determinar responsables ante el deterioro o pérdida de información o su desvío o adulteración.

Por razones históricas parte del equipamiento activo de comunicaciones es de la marca Cisco²⁰, lo que le imprime determinado riesgo a la red al no disponer de soporte para los mismos y ser difícil la actualización de esta tecnología. Esta situación está en proceso de solución migrando a tecnología HUAWEI²¹, que presenta prestaciones similares, encentrándose en funcionamiento en otras entidades del país, con resultados satisfactorios. De hecho, hoy coexisten ambas tecnologías instaladas en la red, siendo similares los procesos de explotación y mantenimiento.

La dispersión geográfica de la empresa conlleva a la existencia de closets técnicos para albergar el equipamiento activo de comunicaciones (*routers*, *switches*, módems) y concentrar los flujos de datos de las diferentes dependencias administrativas y sus correspondientes segmentos de red en su interacción con el Centro de Datos que los atiende. Cada closet debe poseer climatización, acorde a los parámetros establecidos por DTIC-CACSA, con el fin de disponer de una fiabilidad en la prestación del servicio y un aumento de la vida útil del equipamiento, lo que no se garantiza en todos, poniendo en riesgo la estabilidad del sistema.

Entre los medios físicos empleados para la construcción de la infraestructura de comunicaciones se cuentan: los pares de cobre trenzados (UTP) nivel 6 para las redes tipo LAN a 100Mbps, los hilos de fibra óptica multimodo (FO) para distancias mayores no soportadas en UTP y enlaces a 1Gbps y los pares de cobre tipo telefónico para módems de tipo ADSL y distancias aún mayores (2Mbps). En esta infraestructura se comienza a emplear tecnología inalámbrica, al ser autorizada la utilización de las mismas en el país, aunque ya es usada en las redes de las representaciones en el exterior.

Las Unidades en el exterior se adecuan a lo aquí descrito, tanto en sus redes internas, como en lo referente a la comunicación con la casa matriz.

²⁰ **Cisco**: fabricante norteamericano de tecnología informática.

²¹ **HUAWEI**: fabricante chino de tecnología informática.

El sistema operativo de red (NOS) es el denominado Directorio Activo (AD) de Microsoft. Desde esa óptica, la red está compuesta de un conjunto de sitios interconectados, uno para cada país en que existen dependencias, conociéndose, en todo momento, los elementos activos en la red.

Los Sistemas Operativos (SO) desplegados en los servidores (SRVs) son Microsoft Windows 2003 Server Enterprise Edition R2 Service Pack2 y MS-Windows 2008 Server R2. En las estaciones de trabajo (WKS) es empleado algún SO de Microsoft Windows, en sus versiones de Windows XP Professional Service Pack 3 y Windows 2007 Ultimate. En los SO desplegados no se cuenta con sistemas de tipo Open Source, o sea distribuciones Linux (GNU), salvo algunos casos aislados.

El uso de estos sistemas, en las versiones especificadas, garantiza un eficiente manejo de las contraseñas y los permisos de acceso y niveles de privilegios para el uso de la información. Sin embargo, la gran mayoría de los servicios están integrados al sistema operativo de red, dando una facilidad administrativa, requerida por el poco personal técnico existente, pero a la vez, la promiscuidad en la autenticación de los usuarios, constituye una vulnerabilidad, ya que existe un solo factor de identificación para todos los procesos, el nombre de usuario y su contraseña, las que son manejadas de manera irresponsable al ser compartidas o fáciles de identificar.

Existen dos centros fundamentales de datos, el Nodo Central de Servicios Informáticos (NCSI) que radica en las instalaciones de la empresa en HAV-AIJM y el Nodo Alternativo de Servicios Informáticos (NASI), instalado en ubicación de la CACSA en el Vedado. Aunque en cada zona aeroportuaria del país existe un Centro de Datos, desde el punto de vista de las configuraciones, tanto para equipos como para usuarios, las mismas son establecidas centralmente en NCSI. De la misma manera se distribuyen las actualizaciones de los SO de las WKS y SRV, así como las últimas versiones y actualizaciones para el software autorizados para su utilización por DTIC-CACSA. Las configuraciones y actualizaciones para la solución antivirus, son establecidas y distribuidas centralmente en NCSI.

En el NCSI y en el NASI se emplean mayormente SRVs con electrónica o hardware (HW) profesionales (PRO), aunque existen SRV con HW no profesional (NO PRO). La cantidad de SRVs desplegados para soportar los servicios y aplicaciones en todo el país se encuentra en algunas decenas de equipos tanto HW PRO como HW NO PRO.

Por otro lado, la cantidad de WKS se encuentra en el orden de un millar. Una cantidad relativamente alta de ellas se consideran tecnológicamente obsoletas, situación condicionada por los recursos financieros insuficientes que se destinan para una reinversión apropiada en la infraestructura tecnológica. Esto conlleva al empleo de versiones ya obsoletas y sin soporte de actualización para los SO (“*patches*”²²), lo que unido a limitados recursos de cómputo, como la capacidad de memoria, implica bajos desempeños, al coexistir con equipamiento más moderno, lo que ha provocado a su vez un decrecimiento en las prestaciones generales de la infraestructura de red.

En los Centros de Datos de los sitios del interior del país es relevante el uso de SRVs con HW NO PRO, aunque la situación comienza a revertirse con la instalación de SRVs de HW PRO, acorde a las posibilidades de adquisición de estos medios, atendiendo a la expansión que van adquiriendo las redes LAN de estos lugares. En el exterior es común la utilización de SRVs con HW NO PRO, condicionado, fundamentalmente, por las dimensiones de las LAN y las características técnicas de los SRVs, suficientes para la atención a la red y los servicios asociados.

Existen dispositivos móviles como laptops, *netbooks* y *tablets* en diferentes áreas de la empresa. Entre los usos de los mismos se encuentran la realización de reservas de pasajes, en diferentes regiones del país donde no existen Oficinas o Puntos de Ventas y son altos generadores de pasajeros por la densidad poblacional o el asentamiento temporal de estudiantes y adonde se desplazan los especialistas comerciales de las Oficinas que atienden esa región para realizarlas, mientras que en el exterior se utilizan para realizar igual función en los aeropuertos en que opera la aerolínea y no se posee un local de trabajo.

²² **Patches**: conocidos en Cuba como parches del SO.

Este tipo de medio también es utilizado como soporte para los funcionarios y especialistas que viajan al extranjero, que deben cumplir un procedimiento de revisión y adecuación de las configuraciones de dichos equipos, así como del carácter de la información que transportan. Estos dos aspectos se gestionan en la DTIC y en la Dirección de Seguridad y Protección de la empresa a través de la Oficina de Información Clasificada (OCIC), respectivamente. Aunque se elabora un documento certificando que el funcionario o especialista tiene conocimiento de la información que porta y su responsabilidad con ésta y el medio que la soporta, constituye un riesgo para la seguridad del sistema la salida del país de personas con información referente a aspectos del funcionamiento de la empresa, sin control diario de su uso y destino.

Además, la empresa cuenta con Agentes de Generales de Venta (GSA) en varios países, como Islas Martinica (donde también opera como aerolínea), Grecia y Hong Kong (China), para la realización de reservas, lo que extiende el alcance de la aerolínea, pero constituye un riesgo para el SI al poner en manos de terceros el acceso a sistemas de la empresa.

Casi la totalidad de los Puntos de Venta con que cuenta la aerolínea, se encuentran en los aeropuertos nacionales, que son operados por la empresa ECASA S.A., también perteneciente a CACSA y máxima responsable de los servicios aeroportuarios, incluyendo la gestión de la seguridad informática, por lo que los medios de CU en funcionamiento en estos lugares, se rigen por las normas y políticas de ECASA S.A., lo que constituye una puerta trasera de entrada a la red de CU, constituyendo un riesgo.

Desde el punto de vista estructural y con el fin de disponer de seguridad respecto del exterior de la red, la infraestructura que sigue la misma es el esquema tradicional de red interna, DMZ²³ y dispositivos periféricos *firewall*²⁴ para prevenir la intrusión, desde el exterior fundamentalmente. Debe señalarse que al tener a los Centros de datos de

²³ **DMZ (Zona desmilitarizada o red perimetral):** red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. Su objetivo es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir, los equipos locales en la DMZ no pueden conectar con la red interna.

²⁴ **Firewall:** Cortafuegos. Barrera de protección. Enrutador programado que se ubica entre redes y que re-envía, direcciona y filtra flujo de datos que pasan de una red a otra, mediante reglas como direccionamiento, protocolos y puertos, entre otras.

DTIC-CACSA como proveedor de servicios, la red de CU se encuentra relativamente protegida, dados los esquemas de protección de dicho proveedor, debiendo solamente cuidarse de los ataques provenientes de la infraestructura de red del proveedor de servicios de telecomunicaciones ETECSA, requerido por CU para el alcance nacional.

Para lograr esto, en los sitios de CU en el interior del país, se han ubicado dispositivos activos de comunicaciones administrados por CU, con el fin de oscurecer a otros usuarios del proveedor ETECSA, la estructura lógica interna de dichos sitios y limitar su posibilidad de penetración.

Con el exterior las comunicaciones se realizan utilizando conexiones ADSL ²⁵ fundamentalmente, siendo un proceso similar al descrito para las entidades nacionales. También son utilizados los enlaces que se brindan por SITA e INTERNET para las aplicaciones que así lo requieren. Las aplicaciones y sistemas que se utilizan son los mismos, por lo que se cumple lo antes descrito, existiendo también un número importante de WKS obsoletas, coexistiendo con equipamiento moderno, con la consiguiente afectación al trabajo de la red y de las aplicaciones que se explotan.

Son empleadas las tradicionales conversaciones telefónicas, a través de teléfonos fijos, ya sean extensiones nacionales o números privados y la telefonía celular, tanto en el ámbito nacional como en el internacional, así como diferentes enlaces de datos para lograr la comunicación con las unidades nacionales y las representaciones en el exterior. El uso de los medios de telefonía constituye una vía de escape de información, al ser tratados temas con determinado nivel de compartimentación en lenguaje claro y, en ocasiones en presencia de personas ajenas al tema en cuestión, poniendo en peligro la seguridad del sistema de información.

Con el fin de garantizar los aspectos anteriores, se requiere la gestión de canales de comunicaciones, los cuales son provistos por SITA, INTERNET, ETECSA y DTIC-CACSA. La comunicación con las redes globales de comunicación internacionales

²⁵ **ADSL:** *Asymmetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica. Tecnología que proporciona una conexión digital sobre la línea de abonado de la red telefónica, utilizando una banda de frecuencias mayor, por lo que se conoce como conexión de banda ancha. Permite transmitir simultáneamente voz y datos a través de la misma línea telefónica.*

SITA e INTERNET, es mediada a través de la DTIC-CACSA, como proveedor de servicios interno. Para la comunicación dentro de la estructura interna de la subred de CU con sus sitios en el interior del país y los distantes de HAV-AIJM, pero dentro de La Habana, es empleada a ETECSA con su infraestructura de red nacional basada en el protocolo MPLS²⁶.

Las condiciones de las instalaciones civiles donde están desplegadas las tecnologías informáticas son apropiadas para su conservación tecnológica y custodia, garantizando las condiciones ambientales de temperatura y humedad necesarias. En la gran mayoría de los casos son áreas protegidas por la Empresa de Servicios de Protección de la Aviación Civil (ESPAC) o similar en el exterior.

Para acceder a las diferentes áreas de la empresa debe portarse una credencial de identificación, con una clasificación de acuerdo a los niveles de acceso, en dependencia de la criticidad del área. Sus características constructivas son pared de mampostería, ventanas con rejas, puertas con cerradura y dispositivos de sellado en las puertas de acceso, garantizándose las condiciones de alojamiento de los medios técnicos de almacenaje y la gestión de los medios de comunicaciones. Se encuentran garantizados los medios apropiados de extinción de incendios para las TICs, debidamente certificados y revisados periódicamente. En las áreas restringidas existen dispositivos para la detección de incendios (SADI) y detección de intrusos (SACI), así como cerraduras de acceso electrónico.

Existen instalaciones que son compartidas por grupos de trabajo pertenecientes a diferentes entidades de la empresa, pudiendo coincidir en una ubicación física grupos de trabajo de diferentes UEB, así como de las áreas de regulación y control con grupos de una o más UEB. Esto introduce vulnerabilidades al sistema ya que, al constituir un riesgo el manejo de información por diferentes categorías de personal en un área común, se dificulta el control de los medios técnicos del lugar, desde el punto de vista de lograr la correcta segmentación del tramo de la red. Lo mismo ocurre en áreas que

²⁶ **MPLS: Multiprotocol Label Switching. Tecnología para transferencia de datos de alta velocidad y voz digital en una sola conexión.**

son compartidas con otras empresas de la CACSA y que son las que asumen la seguridad, debiéndose compartir recursos de estas entidades y cumplir sus normativas.

En las Oficinas en el exterior las condiciones constructivas son de similar características y se cuenta con medios SADI y SACI actualizados y certificados.

Hay que diferenciar dos tipos de usuarios de las tecnologías, los que las administran y realizan desarrollos (desarrolladores) y los que las usan explotando sistemas y aplicaciones (explotadores). El análisis para el personal que desarrolla es diferente al que las explota. La entrada a la empresa, para formar parte de su personal, para ambos tipos, está basada en un proceso de verificación de la idoneidad desde diferentes puntos de vista.

Para el caso de los explotadores, se confía en los conocimientos que puedan acreditar en la documentación curricular entregada al iniciar el proceso, pero no se realizan exámenes de suficiencia sobre los diferentes aspectos de las tecnologías y los sistemas y aplicaciones con se desarrolla el trabajo, introduciendo cierto grado de incertidumbre sobre la ejecución correcta de programas y que sean entendidas y cumplidas las normas y procedimientos de seguridad de la información, poniéndola en riesgo ante la posible manipulación errónea de opciones de programas. Para los desarrolladores es requisito la certificación, mediante documento acreditativo, de formación superior o técnica en ramas de la informática o especialidades afines.

Asociadas a los desarrolladores se manifiestan vulnerabilidades en el sistema de seguridad informática, al ser insuficiente el personal dedicado a la gestión de la seguridad informática, ocurriendo que implementa y controla medidas técnicas y lógicas de seguridad de las TICs en todos los procesos y sistemas asociados. Esto provoca ineficiencias al enfrentar la solución problemas, dado por falta de segregación de funciones, generando afectaciones a la seguridad, al ocasionar:

- disminución del ambiente de control,
- pérdida de la trazabilidad,
- disminución de la determinación de la responsabilidad,

- debilitamiento de la supervisión del uso adecuado y autorizado de los servicios.

Como una forma de lograr un conocimiento estándar del trabajo con el SI en CU, se imparte un curso de iniciación laboral que contiene instrucción en los aspectos de seguridad de las TICs (STIC) y las políticas establecidas al respecto. En el Contrato Laboral existe un Anexo donde el contratado firma su conformidad y se responsabiliza con los aspectos de la STIC, tanto durante la relación laboral como después del cese de ella.

No obstante, el conocimiento para la utilización de las TICs es bajo, lo que redundo en ocasiones en tipos ingenuos de errores de operación que traen consecuencias negativas sobre la infraestructura tecnológica y la disponibilidad de los datos, lo cual constituye una vulnerabilidad y expone a riesgos la información.

Esta vulnerabilidad es manifiesta en las dependencias del exterior donde se tienen solo explotadores a los que no se verifican, en el momento de la contratación, las competencias digitales que deben poseer, situación que se agrava al tener que ser, según las leyes del país, ciudadanos nativos en un elevado por ciento. Además, son contratados los servicios de mantenimiento y reparación del equipamiento y las redes a empresas o independientes también nativos y, por supuesto, los proveedores de servicios de comunicaciones. Todo lo anterior significa que se pone la información de la empresa, fundamentalmente comercial y financiera, en manos de extranjeros.

2.3 Problemas en la planificación de la Seguridad Informática.

En el informe anual “Evaluación de los riesgos asociados a las vulnerabilidades de las Tecnologías de la Información y las Comunicaciones en la empresa Cubana de Aviación S.A.”, presentado por DTIC para su análisis en el Consejo de Dirección en los últimos 5 años, se aprecia la reiteración de deficiencias y dificultades que indican la no identificación de las prácticas de seguridad de las TICs como necesarias, considerándolas como un gasto que no contribuye a las ganancias de la entidad, obviando que dichas prácticas contribuyen al ambiente de control y por ello están destinadas a la preservación de los valores de la entidad, incluyendo los financieros.

Del análisis de la matriz DAFO de las TICs (*Anexo 5*) se concluye que la temática de seguridad informática no forma parte de la cultura organizacional, no se reconoce en la conciencia de la organización que debe estar alineada con el objeto social de la empresa, por lo que se atiende formalmente al existir disposiciones regulatorias que obligan a ello. No existe conciencia en la organización de la existencia de peligros para la información, asumiéndose la suficiencia de sistemas antivirus para garantizar seguridad, centrándose la atención en la funcionalidad de los medios y no en las funciones que deben cumplir. No es asumida, como necesaria, la inversión frente a la inseguridad.

El enfoque generalizado en la empresa, ante lo relacionado con la seguridad informática, es reactivo y no proactivo, evidenciándose en las acciones ante los incidentes informáticos, sin tomar en cuenta la gestión sistemática de la seguridad como garantía de la no ocurrencia de estos. No se aprecia en el PSI un instrumento de dirección, capaz de regular las desviaciones que se puedan manifestar en lo referente a la información y su manejo y, por tanto, su papel en la toma de decisiones.

Cada área de la empresa debe cumplir las normas establecidas y adecuar, según sus características, los procedimientos, de forma tal que lo relacionado con las TICs sea uniforme y estándar en toda la empresa, lo que incide en los análisis de riesgos a realizar y la definición de las medidas para su gestión, debiendo existir un PSI para cada una de ellas. Esto provoca que una misma entidad o área administrativa pueda contar con más de un PSI o que exista un PSI para diferentes entidades que conviven en una misma ubicación.

Los Jefes de las áreas, incluyendo las unidades en el exterior, no son conscientes de la responsabilidad que tienen en la realización y seguimiento del PSI, no se identifican como los máximos responsables de esta actividad, delegando la ejecución de la tarea y sus actividades asociadas, sin participación alguna durante el proceso de análisis y confección del PSI, alegando la complejidad del tema, que es un aspecto muy técnico y no poseer los conocimientos necesarios para enfrentar la tarea.

Esto, además de evidenciar una pobre preparación sobre el tema, trae como consecuencia que no se encuentran familiarizados con las vulnerabilidades y riesgos tecnológicos e informáticos de su área, no son capaces de detectarlos y controlar el uso de las tecnologías por sus subordinados, por lo que no toman acciones proactivas para su mitigación, impregnando, al sistema de seguridad de la información, de brechas aprovechables por amenazas, ya sean humanas o fenómenos naturales. No identifican la correspondencia directa que existe entre la minimización de vulnerabilidades con la reducción de debilidades del SI.

Es notorio que ninguna de las áreas de la empresa, en el análisis de riesgos que se realiza como parte del Sistema de Control Interno, tenga identificados riesgos relacionados con las TICs y la información, excepto los que se asocian con las amenazas derivadas de los fenómenos naturales, los que carecen de motivo para manifestarse.

Al no contar las entidades con desarrolladores debidamente preparados y avalados para realizar este trabajo y la deficiente competencia en el tema de los directivos, además de la posible coincidencia de más un directivo en un área con necesidad de PSI, estos planes carecen de la objetividad necesaria, restándole importancia y la atención que merece, lo que incide en la calidad de la seguridad y provocando la participación directa, en la elaboración de los PSI, del personal desarrollador, con capacidad para ello, perteneciente a DTIC, convirtiéndolos en juez y parte del proceso, lo que contradice las normas de la seguridad al ser ejecutores y controladores.

Como consecuencia de la diferente localización geográfica de los grupos, el uso de servicios o aplicaciones informáticas específicas, las características del servicio de energía eléctrica, las características del personal que emplea las TICs y el cumplimiento de misiones de nivel prioritario relacionadas con la actividad fundamental de la empresa, se hace necesario realizar análisis diferenciados, arrojando como resultado que son necesarios 47 análisis de riesgos diferentes en toda la empresa, dando como resultado 43 planes para la gestión de la seguridad informática (*Anexo 6*).

Los análisis de riesgos realizados arrojan la existencia de determinadas amenazas que ponen en peligro el sistema de información, comunes a todas las áreas y que se manifiestan frecuentemente o son de conocimiento público, ya sea de manera consciente o no, que pueden ser enunciadas:

- Insuficiencia de respaldo energético ante la falla o falta de calidad de la energía eléctrica suministrada externamente al no contar con sistemas de respaldo suficientes para todas las áreas que lo requieren.
- Insuficiencia de un respaldo energético (UPS ²⁷) a nivel de equipamiento informático de usuario, segmento lógico o Centro de Datos.
- Falta de tierra física en edificaciones aisladas y, en caso de existir la misma, no se encuentra certificada su calidad, impidiendo la protección contra las consecuencias provocadas por fenómenos naturales.
- Dificultades con la climatización requerida para locales tecnológicos y otros que cuentan con una considerable concentración de medios para el trabajo de los usuarios, al existir locales de trabajo con alta concentración de equipos, fundamentalmente computadoras personales, que carecen de equipos de acondicionadores de aire o es insuficiente la temperatura que generan. Medidas de ahorro de energía que van en detrimento de las necesidades de las tecnologías.
- No existen garantías de que las cuentas de usuario posean las características exigidas: privada, personal e intransferible, siendo común el uso de contraseñas de poca fortaleza como nombres propios de hijos, cónyuges o mascotas, fechas de nacimiento, no uso de caracteres especiales (@, #, \$, %, ^, &, *, (,), _, +, {, }, *, -, etc.) y números, así como facilitar contraseñas a otros.
- Uso del servicio de correo electrónico para fines que no están asociados a las funciones de trabajo, siendo usual el intercambio de postales de felicitación por onomásticos, aniversarios y días señalados, el traspaso de fotos, música y video, etc., generalmente utilizando mensajes multi destino o *spam*, provocando

²⁷ **UPS:** *Uninterruptible Power Supply*. Conocido en Cuba como BACKUP. Existe equipamiento con diferentes niveles de potencia, en correspondencia con la necesidad de los medios a proteger.

congestión en líneas de comunicación, llenado de buzones personales y abarrotamiento del espacio de memoria en servidores.

- Aplicaciones soportadas en Microsoft Windows, muchas de ellas en hardware de 32 bits, limitando la migración de los sistemas utilizados hacia versiones soportadas en Código Abierto.
- Alto por ciento de equipamiento en estaciones de trabajo obsoleto y con bajas prestaciones, obligando al uso de versiones de sistemas operativos que ya carecen de soporte de actualización. Además, al encontrarse interconectado con el resto de la red, limita la operación de los equipos más modernos al competir por el uso de los servicios compartidos.
- Como promedio, el personal explotador de las TICs adolece de habilidades y conocimientos respecto de ellas, o hay manifestaciones de intrusismo, provocando errores de operación que repercuten en el equipamiento y los datos.
- Poca identificación de los directivos con la necesidad e importancia de la actividad, relegándola a un segundo plano al percibir solo la funcionalidad de los medios y no sus potencialidades como herramientas para el trabajo.
- Otorgamiento indiscriminado de servicios a los usuarios, por parte de la dirección del nivel correspondiente en la jerarquía administrativa, sin guardar correspondencia con la necesidad acorde a la función que realiza la persona.

En las dependencias en el exterior no se manifiestan de manera frecuente las amenazas relacionadas con la seguridad física, aunque el resto sí se manifiesta y es común a todas que el personal contratado para la gestión contable y otras administrativas, es nativo del país, constituyendo una brecha en la seguridad.

Contar con 43 planes de seguridad informática en la empresa tiene fuerte incidencia en la actualización y seguimiento de los mismos. La actualización desfasada en tiempo de estos, ocasiona que en todo momento exista algún plan desactualizado y que los controles e inspecciones que se realizan se centren en la actualización del plan, no pudiéndose revisar, de manera profunda, las medidas que se prevén para el enfrentamiento a las amenazas y la disminución de los riesgos, por tanto, los análisis de los resultados de los controles no abarcan el alcance que deben tener.

Por otro lado, el gasto de papel y tonel es alto, lograr la firma de todos los implicados en la confección y aprobación del plan en los documentos que se generan, es agobiante y la distribución de los PSI, una vez firmados y registrados, es lenta y en ocasiones ocurre a destiempo durante el año, privando a las áreas de un documento importante para su trabajo, provocando dificultades en el control de su cumplimiento. Esto, a su vez, incide en el ambiente de control y en la percepción de la importancia de la actividad, restándosele la atención que merece.

A los jefes, responsables de la seguridad, les ocasiona contratiempos tener un documento extenso para su revisión y actualización. El personal técnico de las tecnologías no es suficiente en las áreas para llevar esta tarea eficientemente, además de carecer de las competencias necesarias para ello, lo que puede provocar la ocurrencia de incidentes con todas las implicaciones que ocasionan.

La necesaria revisión de las vulnerabilidades que se tienen definidas y los riesgos asociados para su actualización en el tiempo y las condiciones cambiantes del entorno, en muchas ocasiones, no se realizan, limitando la actualización del PSI al cambio de fecha y la actualización de las firmas correspondientes, provocando que se queden desprovistas de medidas, posibles acciones dañinas al SI y perdiéndose la garantía de un SGSI confiable.

Existen amenazas comunes a varias áreas y muchas vulnerabilidades se manifiestan, igualmente, de manera común, como es la carencia de acuerdos con terceras partes y su relación con el SGSI de la organización o que las contraseñas de las cuentas de usuario no posean la fortaleza adecuada y exista promiscuidad en su uso, sin embargo, existen diferentes soluciones para estos problemas similares, implicando, en muchos casos, el despliegue de tecnologías y medios de manera particular, cuando podrían ser de uso común.

La Dirección General, máxima responsable del cumplimiento del PSI, está obligada a planificar disímiles despachos similares para realizar los análisis relacionados con la seguridad informática, máxime teniendo en cuenta que hay tareas asociadas a la seguridad de las tecnologías que son función de áreas específicas, lo que obliga a

éstas a tener también varios encuentros y despachos y planes de seguimiento y control. Esto, unido a los costos que implica mantener la seguridad, provoca en los directivos rechazo a la actividad, faltando la motivación necesaria para enfrentar la tarea.

Al tener que asumir DTIC la ejecución total de la actividad, se ha perdido la perspectiva real del SGSI y las responsabilidades a cada nivel, recayendo sobre esta Dirección todo lo concerniente a la tarea, lo que debilita la seguridad del sistema al ser los ejecutores de la planificación de la seguridad sus propios controladores, restándole objetividad y credibilidad a esta actividad.

Los análisis de riesgos periódicos y las revisiones sistemáticas de los PSI, han permitido elaborar, en el tiempo, documentos en los que se ha concentrado el conocimiento y la experiencia adquiridos, con el objetivo de estandarizar el uso y cuidado de las TICs, unificar criterios y decisiones y garantizar la seguridad de la información, dando lugar a las Políticas para el Sistema de Gestión de Seguridad de la Información (*Anexo 7*) que enuncia las regulaciones a considerar en todas las áreas de la empresa.

Primeramente se elaboraron un grupo de recomendaciones prácticas a cumplir en las entidades en el exterior para la elaboración del PSI, debido a la dificultad de la lejanía, el desconocimiento de los medios con que se contaba en estos lugares y que la atención del sistema se realiza por personal nativo contratado. Estas recomendaciones se fueron transformando según se fue aumentando el conocimiento sobre los mecanismos de trabajo en estas entidades, llegándose a elaborar un grupo de políticas para las UE de CU, en las que se plasmaban la intencionalidad de la acción a seguir, dejando la elección final de la solución a la propia unidad, hasta llegar a las Políticas para el Sistema de Gestión de Seguridad de la Información, que cuenta con 109 políticas, distribuidas en 13 categorías, que se dividen a su vez en 35 sub categorías y abarcan a todas las entidades o áreas de la empresa y son de estricto cumplimiento.

Estos documentos han sido elaborados en el tiempo, a partir de las condiciones que se han tenido en cada momento, como herramientas para el manejo de las necesidades de la seguridad requerida, constituyendo uno la base de partida del siguiente.

Las amenazas y vulnerabilidades asociadas a estas que se identifican en todas las áreas de la empresa, con manifestaciones y probabilidades de ocurrencia similares, le imprimen complejidad a la planificación de la seguridad informática al tomar en cuenta la dispersión de las áreas y su incidencia en el cumplimiento de las funciones de la empresa. La **Figura 9** muestra un resumen mediante un diagrama de Ishikawa.

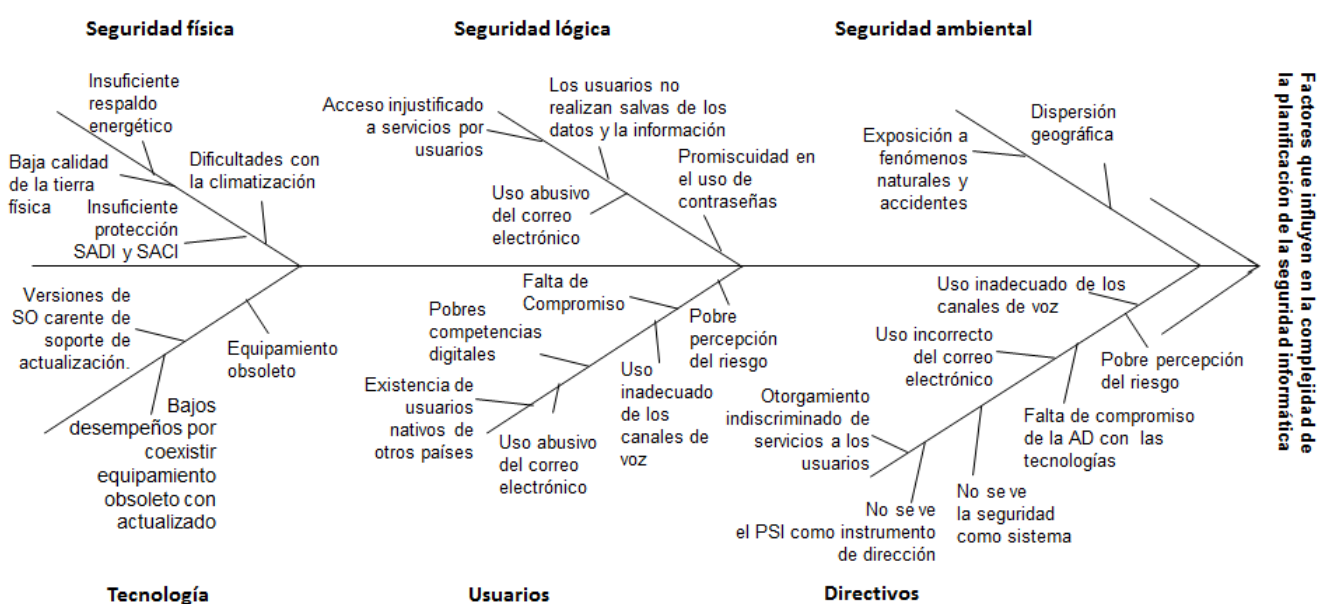


Figura 9. Amenazas y vulnerabilidades asociadas a estas, de manifestación frecuentemente.

Fuente: Elaboración propia

El análisis de las leyes y estándares de seguridad informática existentes en el ámbito nacional e internacional y todo el trabajo realizado por DTIC relacionado con esto, permiten compatibilizar y resumir las amenazas, vulnerabilidades y riesgos que se detectan en la empresa y asumir una planificación centralizada de las medidas para su enfrentamiento y la disminución del impacto.

Capítulo III. Bases metodológicas para la confección de un Plan único de Seguridad Informática.

3.1 Propuesta de solución para la planificación de la Seguridad Informática.

La carencia de un esquema único para la gestión de la seguridad informática, provoca diferentes interpretaciones de la documentación reguladora, lo que trae como resultado diferentes formas de asumir situaciones similares, existiendo diversas variantes de solución o la aplicación de diferentes medidas, para iguales manifestaciones de dificultades, debilitándose el seguimiento y control de las medidas y, por ende, el enfrentamiento a las dificultades.

La presencia de entidades de la empresa en varias regiones del país y diferentes países, le imprime a la planificación de la seguridad informática una singularidad aun mayor, máxime cuando es evidente la falta de identificación con la necesidad de proteger la información y los medios tecnológicos con que se gestiona, debido a la baja percepción del riesgo y la usual falta de prioridad a esta actividad, dificultando la coherencia de medidas para el tratamiento de deficiencias y el enfrentamiento para eliminar o disminuir los riesgos a que se expone el sistema informativo.

La existencia de 43 Planes de Seguridad Informática en la empresa constituye una amenaza de por sí, dada la imposibilidad de mantenerlos adecuadamente actualizados y controladas las medidas para minimizar los riesgos, lo que provoca brechas en la seguridad del sistema.

Las estrategias que se derivan de la matriz DAFO de las TICs para gestionar la seguridad del SI, podrían ser asumidas con un único PSI para toda la empresa, lo que se sustenta en la existencia en Cuba de legislaciones para la regulación de lo concerniente a la actividad de las TICs, basadas en estándares internacionales, unido a que la CACSA ha implementado regulaciones hacia lo específico de la aviación y que en CU existen Políticas de Seguridad, un Reglamento Interno de Red y un Código de Ética.

El PSI es un documento rector que define políticas, medidas y procedimientos para el control y seguridad de la explotación de las Tecnologías de la Información y las Comunicaciones. Como documento, debe reflejar, de manera formal, el Sistema de Seguridad Informática implementado y desplegado, siendo el elemento esencial en el control y explotación de las TICs, confeccionándose de manera que abarque todas las dependencias de CU, ubicadas tanto en el territorio nacional, como en el exterior.

Bastarían a la Dirección General despachos periódicos con DTIC para tener conocimiento de la situación referente a las tecnologías. Por su parte, sería DTIC la encargada de los diferentes despachos por áreas, de manera que se facilita tener criterios sobre los problemas y búsqueda de respuestas a las deficiencias. El personal técnico de las UEB y otras áreas que lo posean, debe ocuparse de vigilar el cumplimiento de las medidas y retroalimentar a DTIC para las actualizaciones y modificaciones pertinentes.

Existe un grupo de necesidades de índole general para la empresa que hacen conveniente una planificación única de la seguridad informática:

- La jerarquización de la actividad de seguridad informática como relevante para la organización y la necesidad de la toma de conciencia por directivos y usuarios de las TICs de su protección y uso correcto, de vital importancia para garantizar la adecuada gestión de la información patrimonio de la empresa.
- La capacitación ordenada y diferenciada que permita a los usuarios de las TICs el uso correcto de las tecnologías, enfatizando en los aspectos que necesite cada cual para el cumplimiento de sus tareas y funciones y que facilite la toma de conciencia colectiva sobre la necesidad de la seguridad informática.
- La preparación integral de directivos, inspectores y controladores para la realización del seguimiento de medidas contra deficiencias.
- Disponer de un documento que permita el análisis y aplicación consecuente y estándar de principios básicos de la seguridad informática para realizar una gestión eficiente de la misma, lo que se hace más necesario por la existencia de

dependencias en el exterior, regidas por leyes y legislaciones de cada país en cuestión

- Enfrentar la existencia de riesgos y vulnerabilidades comunes en varias áreas, con una única medida, con determinadas adecuaciones, como garantía de una misma solución, la facilitación de la toma de decisiones y el control de los resultados.

Por otra parte, se pueden identificar los aspectos que evidencian premisas para la adopción de un PSI único en CU, permitiendo un enfrentamiento a las amenazas con una visión única de las vulnerabilidades y los riesgos asociados y con medidas de alcance global en la empresa:

- El hecho de contar en Cuba con legislaciones para regular el trabajo de las TICs, basadas en estándares internacionales, unido a que la CACSA ha implementado regulaciones hacia lo específico de la aviación.
- Existencia en CU de un ente metodológico y regulador de las actividades relacionadas con las tecnologías de la informática y las comunicaciones, sus usos y cuidados y la introducción de sistemas y aplicaciones.
- Existencia en CU de un Reglamento Interno de Red, un Código de Ética y un incipiente sistema de capacitación a los usuarios de las tecnologías en su uso y cuidado.
- La existencia de Políticas para el Sistema de Gestión de Seguridad de la Información que abarcan a todas las áreas de la empresa.

3.2 Guía para la elaboración de un PSI único.

Es de suma importancia para la organización poseer un sistema de seguridad de la información bien definido y estructurado, apoyado en un sistema de seguridad de las tecnologías de la información sólido y fuerte, que abarque todos los aspectos relacionados con el uso de estos medios y los usuarios que las utilizan, para lograr la seguridad de las informaciones que por ellos se mueve.

Para garantizar uniformidad en los análisis de riesgos, la determinación de vulnerabilidades en las áreas y la definición y ejecución de medidas y tareas para la seguridad de la información que es captada, procesada, almacenada e intercambiada mediante tecnologías informáticas, se hace necesaria una herramienta que permita la organización de la protección del sistema, teniendo como objetivos reducir los riesgos a un nivel aceptable, garantizar confidencialidad, integridad y disponibilidad de la información y cumplir con las leyes y reglamentaciones vigentes.

Disponer de una guía para la organización y ejecución de toda la actividad y tareas asociadas, garantiza un trabajo uniforme en todas las entidades o áreas de la empresa, bajo una dirección única, la de DTIC, dotando al sistema de mayor seguridad y a su documentación de coherencia y lógica únicas, permitiendo una gestión y un control más eficientes.

La función rectora metodológica de DTIC, unido a la administración centralizada de la red y los sistemas y aplicaciones, permite concentrar la administración y gestión de los servicios informáticos en el NCSI, lo que propicia que las Políticas de Seguridad de las Tecnologías de Información y Comunicaciones sean aplicadas centralmente para todas las dependencias de la empresa. Esta implementación técnica fundamenta, conceptualmente, la existencia de un único PSI para todas las dependencias, independientemente de que existan áreas que tengan características específicas.

La estructura del PSI más conveniente al concepto anterior es que el mismo cuente con dos partes, una Sección General y Secciones Específicas, describiéndose en la primera, las características del Sistema de Seguridad Informática comunes a toda la empresa y en la segunda, aquellas características que son particulares a cada área.

En la Sección General se describe:

- Políticas de Seguridad de S-TIC.
- Responsabilidades en el Sistema asociadas a Funciones o Cargos que abarcan toda la empresa.
- Características de los sistemas informáticos y aplicaciones comunes.

- Análisis de Riesgos correspondiente al NCSI.
- Contingencias informáticas comunes.
- Anexos generales.

En las Secciones Específicas se describen, a su vez, aquellas características que son particulares al área (entidad o grupo de entidades o dependencias administrativas), conteniendo:

- Características de sistemas informáticos y aplicaciones específicas.
- Análisis de Riesgos del área.
- Contingencias informáticas específicas.
- Anexos específicos, incluyendo diagramas si fuera necesario para el área.

En una Sección Específica, asociada al NCSI y al NASI, se detallan los equipos, enlaces de comunicaciones y diagramas de red, así como las aplicaciones que se emplean en la empresa.

El alcance del plan pasa a ser ahora global a toda la organización, siendo lo dispuesto en los epígrafes pertenecientes a su Sección General, abarcador a todas las dependencias de CU. En la implementación de su contenido se tienen en cuenta aspectos administrativos, organizativos, legales, tecnológicos y educativos.

Acorde a lo dispuesto en el Decreto Ley 199 y la Lista Interna de la CACSA, el documento contendrá una parte pública y partes con categoría de limitado, indicándose la clasificación de la información contenida en cada página. Las páginas categorizadas como ordinarias serán de conocimiento público para los usuarios de las TICs desplegadas en todas las dependencias de CU. Las páginas categorizadas como confidenciales y limitadas, serán solamente de conocimiento de los directivos y funcionarios con derecho a ello, según los cargos y funciones y su responsabilidad en el proceso.

Los Anexos que contengan los análisis de riesgos del NCSI y de las áreas, esquemas de comunicación y diagramas de red, así como cualquier otro que lo requiera, deben

ser considerados con cierto grado de confidencialidad al contener información que compromete la propia seguridad del sistema, debiendo tener el tratamiento que se establece por la Lista Interna para la documentación clasificada y deben ser guardados y custodiados en la OCIC del nivel central de la empresa, existiendo copia en igual dependencia de las áreas respectivas. De igual manera ocurre con las Secciones Específicas que sea necesario.

El acceso y consulta de esta información solo podrá ser realizada por los directivos y especialistas autorizados y controlado por los mecanismos establecidos para ello. La parte pública del PSI estará publicada en la página web de la organización, accesible, para su consulta, por todos los usuarios de las TICs.

La división en áreas específicas está asociada a diferentes criterios: importancia dentro de la funciones de la empresa, información que se maneja, cercanía en su localización geográfica, similitudes en el uso de sistemas informáticos y comunicaciones o las combinaciones de las anteriores. El criterio fundamental es el referido a la ubicación geográfica, arrojando áreas dentro de Cuba (nacionales) y dependencias en el extranjero (Unidades en el Exterior). Dentro de Cuba, a su vez, se subdividen en dependencias en La Habana y Unidades de Venta en el interior del país.

Cada área, incluyendo las que radican en el exterior, bajo la supervisión de DTIC, realizaría el análisis de las posibles amenazas que afectan el sistema informático, la definición de los aspectos que constituyen puntos débiles en el sistema, una estimación de las pérdidas que esas amenazas podrían ocasionar y un estudio de las probabilidades de que ocurran. A partir de este análisis, se diseña el esquema de seguridad en el que se establecen las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos, si se llegaran a producir.

La existencia de un único documento permite la coherente aplicación de las Políticas de Seguridad asumidas para la empresa, sin diferencia de interpretaciones y constituye un mecanismo para garantizar la aplicación y el uso de estrategias conocidas como básicas en seguridad informática (ECURED, 2014. Disponible en: http://www.ecured.cu/index.php/Seguridad_Informatica. Recuperado el 08/03/2014)

- Mínimo privilegio: se otorgan los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado.

Todos los usuarios a todos los niveles, gozan de permisos de acceso a los servicios y a la información en correspondencia con sus funciones y responsabilidades, evitándose accesos indebidos a sistemas y aplicaciones que no sean de su competencia, así como a zonas de resguardo de información.

Solo el personal perteneciente al área de administración de redes realiza la gestión de estos permisos, los que son controlados periódicamente por los especialistas del área de seguridad informática.

- Acceso: la decisión sobre lo que se puede hacer corresponde solamente a la Dirección.

Los directivos de cada área son los responsables de solicitar a DTIC, para cada subordinado que opera las TICs, los accesos que necesite para su trabajo, mediante modelos habilitados al efecto, en los que se fundamentan las solicitudes, en correspondencias con las funciones del puesto de trabajo. La aprobación de estos modelos, según el caso, puede implicar diferentes niveles de verificación y aprobación, desde el área de Capital Humano, hasta la máxima dirección de la empresa.

Se considera que todo lo que no esté expresamente permitido está implícitamente prohibido.

- Defensa en profundidad o multinivel: se implementan mecanismos de defensa a los diferentes niveles de los procesos y servicios.

La seguridad del sistema no depende de un solo mecanismo.

Utilización de controlador de dominio principal y varias réplicas para el control de funciones y servicios, con actualizaciones periódicas y la salva de 2 configuraciones anteriores.

Solución antivirus con administración centralizada, con servidor maestro en NCSI y esclavos o hijos donde proceda.

Descarga permanente de actualizaciones o *patches* de SO de manera centralizada.

Autenticación mediante contraseñas para acceso a servicios.

Control de uso de contraseñas fuertes para servicios críticos.

- Diversidad: utilizar diferentes mecanismos de defensa para limitar el alcance de los ataques y reducir los efectos de errores.

Segmentación de la red por tramos, utilización de servidores Proxy de cara al exterior de la red central, uso de firewall (filtrado de paquetes) entre dispositivos, implementación de DMZ entre redes.

Balanceo de carga de conexiones entrantes.

Disponer de un plan general de mantenimiento y actualización de estos dispositivos, tanto el software como el hardware.

- Punto de choque o de control centralizado: tener una vía única de entrada para el control y la supervisión.

Alinear todos los mecanismos de seguridad, de modo que los usuarios tengan que pasar por ellos para acceder al sistema

El monitoreo centralizado de todo el sistema permite la detección de anomalías y la administración centralizada de medidas de enfrentamiento.

Se facilita poder realizar controles y comprobaciones a todo el sistema de manera planificada y por prioridades.

- Eslabón más débil: enfatizar la protección, el control y la supervisión del punto más vulnerable o débil del sistema.

Se pueden determinar los puntos de mayor vulnerabilidad en el sistema, permitiendo la posibilidad de dedicar los esfuerzos y recursos, para cada caso, de manera eficiente y eficaz, implementando una protección escalonada que redunde en la del sistema en su totalidad.

- Proporcionalidad de las medidas de defensa: correspondencia de la importancia del objeto a proteger con el nivel de riesgo que existe para el mismo.

Es posible definir prioridades en todo el sistema, destinando esfuerzos y recursos en dependencia del nivel de riesgo y la importancia del objeto para el sistema en un momento dado.

- Participación universal: participación activa y consciente en el uso y despliegue del sistema de seguridad por parte de todos los usuarios.

La seguridad de todo el sistema pasa a ser una necesidad de todos los participantes en el mismo, obligando a que se conozcan todos los aspectos relacionados, independientemente de que se manifiesten o no en su área de acción.

- Uso del sentido común: no deben violarse las normas elementales.

Mediante una capacitación ordenada y sistemática, fomentar la conciencia de la necesidad de la seguridad.

Todo lo establecido para la seguridad del sistema es de cumplimiento por todos los participantes, independientemente del nivel de manifestación en áreas específicas y el lugar donde se encuentre.

Posibilidad de aplicación del Código de Ética para todos de manera similar, compartiendo la responsabilidad por la seguridad del sistema.

- Definiciones asociadas a la temática: la documentación que se elabora contiene todas las definiciones y notas aclaratorias que sean necesarias para su mejor comprensión, utilizando un vocabulario común.

Se define, de manera específica y por niveles, las responsabilidades y, en su caso, las funciones, de los implicados directos con el sistema de seguridad de las tecnologías, lo que regula que la existencia de especialistas y técnicos informáticos en diferentes grupos funcionales de la empresa, lleve a que se asuman tareas que no competen y que se dejen de cumplir otras que si corresponden y que surja la tendencia en los usuarios de estas áreas, de deslindar los temas de seguridad del trabajo cotidiano, realizando adecuaciones muy a lo interno del área y desconociendo regulaciones establecidas para cumplimiento de todos. Del cumplimiento consecuente y responsable de estas funciones depende, en gran medida, la correcta gestión del sistema de seguridad.

También son definidas las responsabilidades y funciones relacionadas con la seguridad informática, de los directivos y especialistas del área de Seguridad y Protección, que responden por la seguridad de la información, esté o no contenida en soportes informáticos y por la seguridad física de las instalaciones, en lo que respecta, entre otros aspectos, al acceso físico a las mismas y la protección contra incendios.

Las medidas de seguridad, tanto desde lo relativo a la seguridad física, como a la lógica y ambiental y la operatividad, pueden ser descritas de manera estándar para todas las áreas, dejando claramente definidos los mecanismos de salvaguarda de la información y su restaura.

Las medidas referidas a estos aspectos garantizan la continuidad del negocio de la empresa, de manera que sea posible la recuperación de información, en caso de eventos naturales o accidentes y su disponibilidad para continuar su adecuada gestión y garantizar la tomas de decisiones. Se posibilita la realización de simulacros o ejercicios, parciales y generales, de restaura de la información para la comprobación real de garantía de la continuidad del negocio.

Las áreas que comparten el mismo espacio físico no pueden eludir la participación y la responsabilidad en la confección y seguimiento del plan, debiendo participar de manera conjunta y haciendo cada una sus aportes al respecto, pudiéndose abarcar todo el espectro de situaciones y necesidades, evitando omisiones.

Se facilita el monitoreo del uso de sistemas, aplicaciones y servicios, así como las actualizaciones de los mismos y la implementación de otros nuevos. La necesidad informática de un área puede ser generalizada a otras, si fuera necesario, de manera rápida y segura, al contar con las características de cada una, las amenazas que la hacen peligrar y las vulnerabilidades que presenta, permitiendo accionar de manera precisa para lograr estandarización.

Se hace posible una capacitación escalonada, diferenciada y por niveles de participación en el SI, de todos los directivos y usuarios de las tecnologías, lo que permite incidir de manera directa en la toma de conciencia de la responsabilidad de cada participante en el proceso informativo y elimina los baches que se presentan hoy en el conocimiento sobre el tema.

El conocimiento por todos de las amenazas más comunes y las imprescindibles acciones previstas para su enfrentamiento, permiten elevar la preparación para este desafío, de manera que pueda asumirse de manera coordinada y uniforme,

disminuyendo el impacto de los riesgos asociados a accidentes y fenómenos naturales, inevitables y en ocasiones inesperados, con catastróficas consecuencias y con diferentes formas de manifestarse en todo el territorio que cubre la red de CU. Esto permite definir prioridades para la atención de los problemas y la movilización de fuerzas y la concentración de presupuestos para la solución de los más acuciantes.

Para los casos de áreas de la empresa que comparten la ubicación física en locales de otras entidades empresariales y supeditan la seguridad a lo establecido para la gestión de la seguridad informática en estos lugares, se logra la aplicación de regulaciones y medidas similares para todos, facilitando el intercambio con los gestores y los acuerdos al respecto.

Un requisito esencial para el funcionamiento correcto y estable del sistema, lo constituye estandarizar los procedimientos claves de trabajo para una actividad segura de las TICs. Estos procedimientos son de obligatorio cumplimiento por cada instancia, según les competa y deben ser adecuados para su ejecución en cada entidad de la empresa, lo que permite generalizar las acciones a seguir para el trabajo, garantizándose así la uniformidad de las acciones y posibilitando poder realizar análisis e investigaciones ante la ocurrencia de eventos indeseados, ya sean de manera consciente o no.

Los procedimientos se encuentran en un anexo general y cada uno define su alcance y los responsables de su ejecución, evitando ejecuciones diferentes de procesos similares y por tanto, logrando un trabajo estándar y coordinado. Las áreas que necesiten adecuar algún procedimiento, motivado por sus características, lo harán en un anexo específico, debidamente referenciado y aprobado por los directivos y especialistas de DTIC.

Los procedimientos claves de trabajo para garantizar la uniformidad en la ejecución de las tareas incluidas en el PSI único, son los siguientes:

1. Proceso de cuarentena. Se asegura que los ficheros y documentos que se pretenden utilizar para el trabajo, no contengan programas malignos, mediante la

realización de pruebas en ambientes simulados y similares a los reales en que serán utilizados.

Se garantiza que las pruebas se realicen durante tiempos y condiciones similares, independientemente del lugar de realización de las mismas.

2. Protección contra programas peligrosos. Se estandarizan los pasos a seguir para la protección contra programas dañinos, evitando omisiones y violaciones involuntarias.
3. Movimiento del equipamiento informático y de comunicaciones. Es reglamentada la forma en que se mueven las TICs por las áreas de la empresa, respondiendo a las necesidades de mantenimientos, reparaciones, bajas y asignaciones, bajo las condiciones de seguridad previstas en cada caso y encaminadas a prevenir la pérdida de información.

Se retroalimenta al sistema contable para el control de los activos.

4. Otorgamiento de acceso a las TICs. Se controlan los accesos a las tecnologías de información y recursos informáticos, según lo reglamentado por el Procedimiento de Calidad correspondiente y que es actualizado según las revisiones anuales del mismo, garantizando las actualizaciones necesarias por cambios en las tecnologías.
5. Asignación de derechos y permisos. Se reglamenta cómo efectuar la asignación de derechos, garantizándose que los usuarios obtengan los permisos y privilegios que le corresponden, según aval de los directivos del área.
6. Salvas de respaldo. Se reglamenta el mecanismo de salvas de respaldo de la información contenida en los servidores, así como la que se encuentra en las estaciones de trabajo.
7. Mantenimiento y reparación. Se reglamenta cómo efectuar los mantenimientos y reparaciones y por quién, en cada caso.

Las actualizaciones y modernizaciones de los medios se realizan de manera centralizada, según el plan de necesidades que se elabore al efecto, teniendo en cuenta los reportes de necesidades de todas las áreas.

8. Inspecciones. Se define la realización de inspecciones, su periodicidad y los ejecutores de las mismas, así como el formato de los análisis a realizar.

Las inspecciones tienen carácter sistemático y sorpresivo y abarcan todas las áreas de la empresa.

9. Análisis de las trazas de navegación por internet. Se establecen los mecanismos para detectar cualquier violación de las normas establecidas para ese servicio, por los usuarios que tienen autorizada la navegación o el acceso, por esta vía a entidades internacionales, para la realización de transacciones financieras.

La seguridad informática, no depende solo de la implementación de los medios tecnológicos y las medidas de seguridad, se requiere permanentemente monitoreo y mantenimiento. De ahí la necesaria retroalimentación de las áreas para mantener actualizadas las medidas a ejecutar, lo que se logra con los contactos periódicos para el seguimiento de las tareas, pudiéndose concentrar soluciones comunes a diferentes áreas.

Las unidades en el exterior se hacen conscientes de su participación en los procesos de la empresa y podrán disponer de una forma de trabajo que puede ser impuesta, por elementos contractuales, a los terceros que asumen los servicios, al ser disposiciones generales de la empresa de estricto cumplimiento, incidiendo de manera directa en la ejecución de actividades críticas, como el resguardo de la información, evitando que ésta sea manipulada por elementos ajenos. Los trabajadores de las unidades que son nativos del país, estarían en la obligación de cumplir con todo lo que se estipula, disminuyendo los riesgos asociados al conocimiento y manejo de información de la empresa.

Un PSI único garantiza el estado de actualización del plan, elaborado con la participación de todas las partes interesadas en el proceso de gestión de la seguridad, partiendo de la identificación de amenazas y vulnerabilidades y las posibles consecuencias de manifestarse alguna, lo que es visto y definido en cada área por los propios usuarios con la participación de DTIC, que concentra y concilia toda la información, logrando tener una visión única de la situación general de la empresa y la que se tiene en cada dependencia, asegurándose soluciones escalonadas, coherentes y estándares para el enfrentamiento.

La realización de controles e inspecciones se facilita, al poseer un único mecanismo para ello, aplicable a todas las áreas de la empresa, unificándose los mecanismos de control locales de las áreas y las medidas disciplinarias correspondientes a violaciones de lo estipulado.

Se hace factible la preparación continua de directivos y especialistas que responden por la seguridad y el fomento de un pensamiento único respecto a las TICs entre los usuarios de las mismas, enfatizando en la obligatoriedad del cumplimiento de medidas como el uso de contraseñas seguras y el respaldo de la información con que se trabaja.

El mecanismo de respaldo de la información es similar para todas las áreas, con las copias de seguridad requeridas, sin obviar pasos ni confundir destinos, permitiendo contar siempre con información actualizada y garantizado, de ser necesario ante la ocurrencia de incidentes, la restauración de la misma y la continuidad del trabajo de la entidad.

3.3 Proceso de planificación de la seguridad informática.

La definición de una guía para el trabajo de planificación de la actividad de seguridad informática es garantía de uniformidad en las tareas y estandarización de soluciones, a la vez que la existencia de las Políticas para el Sistema de Gestión de Seguridad de la Información asegura que se tenga una visión única de las regulaciones y medidas a aplicar para la protección de activos de suma importancia para la organización, la información y los medios tecnológicos en que se gestiona.

Se logra establecer un proceso de planificación, centrado en un objetivo concreto y común para toda la empresa, eliminándose que en las áreas se releguen a segundo plano tareas relacionadas con la actividad. Se identifica una política de seguridad en la organización, lo que implica un alto compromiso, fortaleciéndose el ambiente de control de la empresa y logrando coherencia con el Sistema de Control Interno. (*Figura 10*).

Las responsabilidades con el sistema están identificadas y definidas a todos los niveles, estableciéndose los responsables y participantes en la elaboración, ejecución y actualización del PSI, bajo la dirección metodológica de la DTIC.

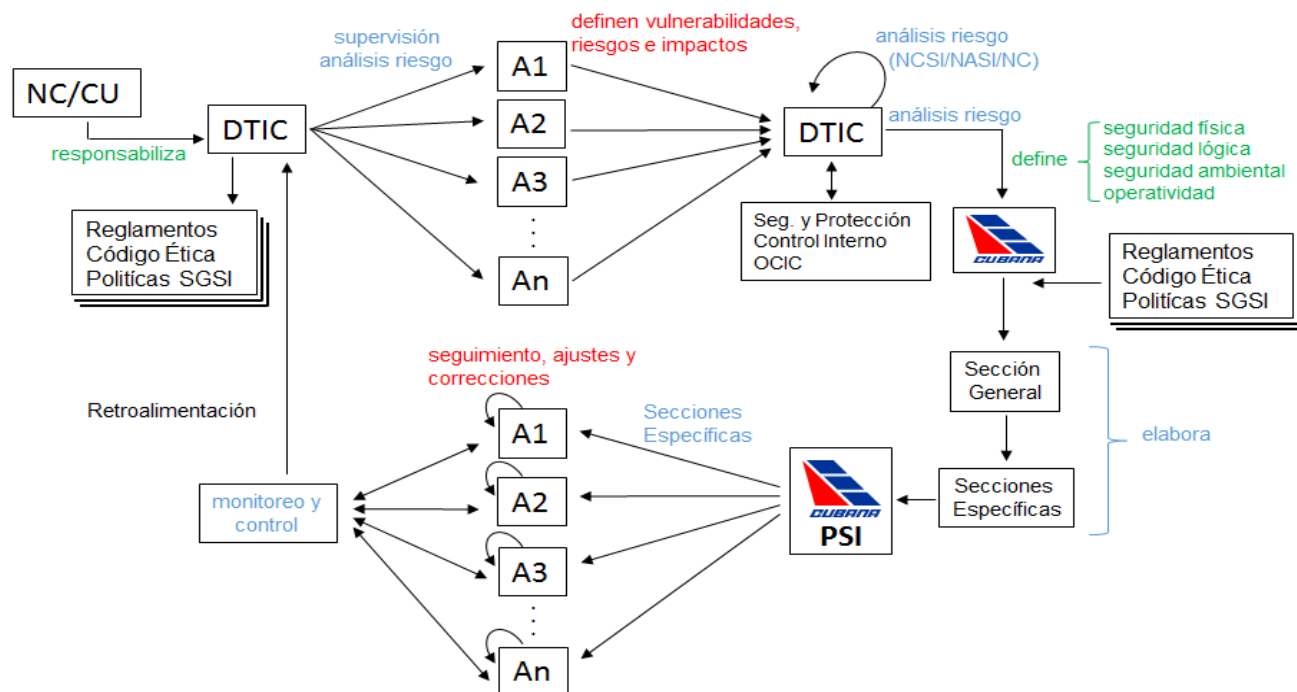


Figura 10. Proceso de planificación de la Seguridad Informática.

Fuente: Elaboración propia

Es enunciada, de manera explícita, la información que debe quedar registrada para su utilización en controles e inspecciones, así como en el esclarecimiento de hechos extraordinarios.

Poder disponer de un sistema de seguridad bien elaborado permite que la organización pueda trabajar de manera confiable y estable, siendo evidentes los beneficios que se obtienen:

1. Se concentra en una sola entidad, DTIC, todo lo relacionado con la gestión y control de la seguridad informática.

2. Se garantiza la existencia de un plan actualizado y su ajuste a la legislación vigente y de estricto cumplimiento por todas las áreas de la empresa. El PSI como instrumento de dirección.
3. Alcance global de la seguridad de la información, abarcando todas las dependencias de CU, ubicadas tanto en el territorio nacional, como en el exterior.
4. Las tareas relacionadas con la seguridad informática son incorporadas al Plan de Trabajo de la empresa y chequeadas por la alta dirección.
5. Coherente aplicación de las Políticas de Seguridad asumidas para la empresa, sin diferencia de interpretaciones, constituyendo un mecanismo para garantizar la aplicación y el uso de estrategias.
6. Se contribuye a reforzar el Sistema de Control Interno al dar coherencia a la seguridad y mejorar el ambiente de control.
7. Se elimina la dualidad de funciones de los encargados de la seguridad informática, al pasar a ser supervisores en la confección del PSI y poder asumir solo las responsabilidades de controladores.
8. Se facilita contar con un plano de análisis más amplio, al poder realizar análisis de vulnerabilidades con enfoque global para toda la empresa y no individualmente por área
9. Facilitación de la toma de decisiones y el control de los resultados.
10. Visión única de la situación general de la empresa y de cada dependencia, asegurándose soluciones escalonadas, coherentes y estándares para el enfrentamiento.
11. Posibilidad de realizar controles integrales a la seguridad informática, de manera centralizada y con la participación de todas las partes.
12. Único mecanismo de inspecciones y de medidas disciplinarias correspondientes a violaciones de lo estipulado.
13. Participación colectiva en la definición de las amenazas, vulnerabilidades y riesgos y las medidas de enfrentamiento, contribuyendo a que se perciba y se asuma el riesgo. Enfrentamiento colectivo a las dificultades.

14. Permite tomar conciencia de la necesidad de la seguridad. Compromiso compartido por directivos y usuarios.
15. Uniformidad en los análisis de riesgos para determinar las vulnerabilidades en las áreas y en la definición y ejecución de medidas y tareas para la seguridad de la información que es captada, procesada, almacenada e intercambiada mediante tecnologías informáticas.
16. Enfrentamiento único a vulnerabilidades y riesgos comunes a varias áreas. Garantía de que no existan vulnerabilidades sin medidas de protección, ni riesgos sin medidas de enfrentamiento.
17. Definición de responsabilidades y funciones de los implicados directos con el sistema de seguridad de las tecnologías de manera específica, estándar y por niveles.
18. Descripción estándar de medidas de seguridad física, lógica y ambiental para todas las áreas.
19. Definición de medidas operativas de salvaguarda de la información y su restauración para todas las áreas, dejando claramente definidos los mecanismos, sin obviar pasos ni confundir destinos, permitiendo contar siempre con información actualizada.
20. Garantía de la continuidad del negocio de la empresa, al ser posible la recuperación de información, en caso de eventos naturales o accidentes y su disponibilidad para continuar su adecuada gestión y garantizar la toma de decisiones. Posibilidad de realizar simulacros de preparación.
21. Incremento de la eficiencia del monitoreo del uso, actualización e implementación de sistemas, aplicaciones y servicios.
22. Preparación y capacitación continua, organizada y escalonada de directivos y usuarios de las TICs, fomentando el pensamiento único respecto a la seguridad de las mismas.
23. Elevación de la preparación para el enfrentamiento de las amenazas más comunes al ser del conocimiento de todos.
24. Definición de prioridades para la movilización de fuerzas y concentración de presupuestos para la solución de problemas.

25. Estandarización paulatina y ordenada de las tecnologías destinadas a la gestión de la información, en correspondencia con los presupuestos destinados para ello.
26. Estandarización de procedimientos claves para el trabajo seguro de las TICs, mediante regulaciones de uso obligado a todos los niveles.
27. Se transforman las vulnerabilidades y riesgos locales en generales, siendo de interés de todos, su eliminación o minimización, fortaleciéndose la seguridad informática en la empresa.
28. Las unidades en el exterior disponen de una forma de trabajo que puede ser regulada, por elementos contractuales, a los terceros que asumen los servicios.

A pesar de los ventajosos beneficios que se evidencian, es posible identificar un grupo de limitaciones que continúan manifestándose, lo que indica que es preciso la vigilancia constante para lograr minimizar el impacto de los riesgos a los que se expone el sistema de información. Entre estas limitaciones se destacan las siguientes:

1. Se mantiene la dispersión geográfica de la empresa, con posibilidad de que se incremente al ser factible el crecimiento de la empresa y se establezcan nuevas oficinas en el exterior.
2. No se garantiza una definición del Sistema Informativo correcta, ajustado a las necesidades informativas de la organización.
3. La existencia de un PSI único permite el enfrentamiento multilateral y centralizado de las vulnerabilidades, pero no su eliminación o disminución.
4. Se mantienen las áreas que comparten la ubicación física en locales de otras entidades empresariales y siguen supeditadas a la seguridad de estas.
5. La capacitación organizada, escalonada y por niveles no garantiza que sean utilizadas las TICs y los servicios asociados a estas, de manera eficiente y racional.
6. No se elimina la promiscuidad en la definición y uso de contraseñas (contraseñas fuertes, privadas, personales e intransferibles) al ser una decisión del usuario.

7. No garantiza que el resguardo de la información que se encuentra en los puestos de trabajo sea responsable, con la periodicidad requerida y en los medios destinados para ello, al depender de los usuarios y el nivel de control de los directivos.
8. No se elimina la posibilidad de ocurrencia de ataques piratas o mal intencionados, por parte de agentes externos, ni la actuación irresponsable de usuarios descontentos e inconformes.
9. Los servicios para intercambio de información son los mismos, por lo que se mantienen los riesgos asociados a estos, como son la interrupción, la interceptación, la modificación o la invención de información.
10. No se garantiza la asignación de presupuestos suficientes para enfrentar la actualización de las TICs.
11. Poseer un único mecanismo de control y enfrentamiento a las deficiencias no garantiza que estas sean eliminadas o minimizadas al estar en el ámbito de actuación de las personas.
12. El diseño del sistema de gestión de la información continua siendo dependiente del sistema informativo de la organización, por lo que una incorrecta definición del primero puede llevar a una incorrecta gestión de la seguridad informática.

Con un PSI único se logra concentrar en una sola entidad, DTIC, todo lo relacionado con la gestión y control de la seguridad informática, presentando a la Dirección General una visión amplia y abarcadora de la situación en las dependencias de la empresa, logrando la estandarización de los medios técnicos, el uso consiente y adecuado de presupuestos y el cumplimiento de las regulaciones sobre el uso de las TICs de manera uniforme, garantizando la continuidad del negocio.

El control y administración eficiente de las TICs y los recursos a ellas asociados, genera beneficios claros: ahorro de recursos, servicios estables y seguros, desarrollo tecnológico planificado, capacitación y superación de recursos humanos gradual y según las necesidades, sin olvidar la información en sí, núcleo de todo sistema automatizado y elemento principal para una toma de decisiones oportuna y confiable (Solórzano, 2006).

Conclusiones.

- El estudio de las fuentes relacionadas con la gestión de la seguridad informática, no permite asumir un esquema único, universalmente aceptado, para ejecutar su planificación, debido a la gran diversidad de normativas y modelos existentes y las diferentes propuestas para su ejecución.
- Cubana de Aviación S.A. presenta un alto grado de dispersión geográfica, debido a la existencia de gerencias y representaciones en casi la totalidad del territorio nacional y en 20 países haciendo compleja la planificación de la seguridad informática, no solo en Cuba, sino en el exterior, lo que se agrava con las especificidades de cada país.
- Las representaciones en el exterior contratan la atención a las TICs y los servicios asociados, a empresas del país, lo que pone en riesgo el sistema de información en estas entidades, al permitir que terceros tengan acceso a los medios y recursos informativos de la empresa, sin que exista un documento legal que les imponga condiciones y restricciones.
- Se encuentra definido el sistema de información de la empresa, siendo su soporte fundamental las tecnologías de la información y las comunicaciones, por lo que el sistema de seguridad informática está dirigido, fundamentalmente, a la protección de información sensible de la organización.
- Existen actualmente en la empresa 43 PSIs asociados a las diferentes áreas, según su ubicación geográfica, lo que conspira contra la propia seguridad, dadas las brechas que abre en el sistema ante la imposibilidad de que puedan ser controlados y actualizados en un tiempo razonable para mantener vigencia.
- La elaboración de los PSI de las áreas por especialistas de la Dirección de Informática y Comunicaciones, los convierte en jueces y parte de la seguridad, perdiéndose la necesaria contrapartida en controles e inspecciones.
- Se identificaron las principales dificultades y deficiencias que presenta CU que hacen compleja la planificación de la seguridad informática por su manifestación similar en diferentes áreas físicas, dado en la seguridad física, lógica y ambiental, las características de las tecnologías y las personas que las utilizan.

- El estudio realizado permitió demostrar la existencia de condiciones para la elaboración de un PSI único en Cubana de Aviación S.A.
- Las bases metodológicas propuestas en este trabajo permiten asumir un esquema para la planificación única de la seguridad informática en CU y disponer de un documento para el análisis y aplicación estándar de los principios básicos de la seguridad informática para enfrentar riesgos y vulnerabilidades comunes con medidas similares, resolviendo la contradicción de ser DTIC juez y parte de la seguridad, fortaleciéndose el ambiente de control de la empresa y logrando una interacción fluida y segura con el Sistema de Control Interno.
- Los beneficios que se logran al tener la seguridad de la información alcance global, poder disponer de un documento para el análisis y aplicación estándar de principios básicos de la seguridad informática y eliminar la dualidad de funciones de los encargados de esta actividad, dan coherencia a la seguridad y mejoran el ambiente de control en la empresa.

Recomendaciones.

1. Estudiar y analizar, en el colectivo de directivos y especialistas de DTIC y el resto de las áreas que cuentan con personal para atención a las TICs, la propuesta presentada para, de ser necesario, adecuarla.
2. Presentar, una vez tomada la decisión final, la propuesta a DTIC-CACSA para su aprobación y presentación al Consejo de Dirección de la empresa para su estudio y aprobación a ese nivel y comenzar la implementación.
3. Actualizar los planes de capacitación de los trabajadores de la empresa, en materia de seguridad de las tecnologías de la información, con las definiciones y conceptos que se definen.
4. Proponer al Consejo Científico del CETED, que se aborden en el Curso Informática para dirigentes del Plan de Estudio de la Maestría en Dirección, los aspectos relacionados con la seguridad de la información y las TICs y las normativas de país al respecto, que son tratados en el trabajo.

Bibliografía.

Benemati, J., Lederer, A, Singh, M. (1997) Changing information technology. *Information Technology Management*, 31, (5), 276-288.

Blanco Encinosa L., (2001), Información, conocimiento y economía: reflexiones sobre el valor y el costo de los recursos informativos. *Economía y Desarrollo* 129, (2), 79-87

Cardona, O.D.; Hurtado, J. E.; Duque, G.; Moreno, A.; Chardon, A.C.; Velásquez, L.S. & Prieto, S.D. (2003). *La Noción de Riesgo desde la Perspectiva de los Desastres: Marco Conceptual para su Gestión Integral*. BID/IDEA Programa de Indicadores para la Gestión de Riesgos, Universidad Nacional de Colombia, Manizales.

Carr, Nicholas G., (2003), *IT Doesn't matter*, Harvard Business Review

Chiavenato, Adalberto (2006), *Introducción a la Teoría General de la Administración*, México: McGraw-Hill Interamericana.

Colectivo de Autores, (2008) *Aspectos básicos de la seguridad y defensa nacional de Cuba*, Colegio de Defensa Nacional.

Colectivo de Autores (2015) Informes y otros documentos de trabajo de la Dirección de Informática y Comunicaciones de Cubana de Aviación S.A., 2010, 2011, 2012, 2013, 2014 y 2015

Colectivo de Autores, (2001) *Seguridad en UNIX*, FACENA. Disponible en <http://exa.unne.edu.ar>. Recuperado: 26/02/2013

Czinkota Michael & Kotabe Masaaki, (2001), *Administración de Mercadotecnia*, Thomson Learning, Segunda Edición.

Díaz Duarte D., (2001), Toma de decisiones: el imperativo diario de la vida en la organización moderna. *Acimed* 2005; 13 (3). Recuperado el 15/08/2014 de http://bvs.sld.cu/revistas/aci/vol13_3_05/aci09305.htm

DRAE, 23^{ra} edición (2014) Disponible en <http://www.rae.es/diccionario-de-la-lengua-espanola/la-23a-edicion-2014>

Ferrell O. C. & Hirt Geoffrey, (2004) *Introducción a los Negocios en un Mundo Cambiante*, México: McGraw-Hill Interamericana Cuarta Edición.

FORRESTER, J.W. (1968): *Industrial Dynamics*. MIT Press, Masachusets.

Gómez Vieites, Álvaro (2011). *Enciclopedia de la Seguridad Informática*. 2ª Ed. actualizada ISBN: 9788499640365, 2011, Ra-Ma Editorial, S.A.

Hellriegel, D., Slocum, J. & Woodman, R. (2004). *Administración*. España. ITP.

Horton, F. W. *Information Management Workbook*. Washington: Information Resource Press, 1985.

Horton, F. W. & Mugge, C. Hacknotes (2003). *Network Security Portable Reference*. McGraw Hill.

ISO/IEC 13335 (2004), *Guías para la gestión de la seguridad de TI*. Disponible en <http://iso25000.com/index.php/normas-iso-25000>. Recuperado: 15/08/2014

ISO/IEC 17799 (2005), *Tecnología de la información – Técnicas de seguridad*. Versión electrónica. Disponible en <https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf>. Recuperado: 15/08/2014

ISO/IEC 25000 (2005), *Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SquaRE*. Disponible en iso25000.com/index.php/normas-iso-25000. Recuperado: 15/08/2014

ISO/IEC 27001 (2005), *Information technology — Security techniques — Information security management systems — Requirements*. First edition. ISO copyright office. Switzerland.

Laudon, K. C. & Laudon, J. P. (2004) *Sistemas de Información Gerencial*, México: Editorial Pearson Education Inc. Séptima Edición

Lineamientos de la Política Económica y Social del Partido y la Revolución (2011), Folleto publicado en www.cubadebate.cu

Malinowski, Bronislaw K. (1944). *Una teoría científica de la cultura*. Barcelona Edhasa 1970

Marrón Duque de Estrada, Rolando, (2010). *Cubana de Aviación El instrumento elegido (1929-1961)*, La Habana, Libro publicado en homenaje al 80 Aniversario de la fundación de Cubana de Aviación

Maslow, Abraham (1943). *A Theory of Human Motivation*, Disponible en <http://psychclassics.yorku.ca/Maslow/motivation.htm>. Publicación original en Psychological Review, 50, 370-396. Consultado: 09/12/2013

Meléndez Carballido, Rogelio & Pérez Calderón, Manuel José (2010), *El régimen jurídico de la seguridad informática en el sistema empresarial cubano. Una visión actual*. Disponible en <http://www.eumed.net/libros-gratis/2010a/671>

Mifsud, E., (2012), *Introducción a la Seguridad Informática*, Disponible en <http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica>

Moliner, M., (1988), *Diccionario de uso del español*. Madrid: Gredos

NC ISO/IEC 17799:2007, (2007), *Tecnología de la información — Código de buenas prácticas para la gestión de la seguridad de la información (ISO/IEC 17799: 2005, IDT)*. Oficina Nacional de Normalización, 1ra Edición abril 2007

Ochoa Ovalles, S. & Cervantes Sánchez, O. (2012), *Seguridad informática*, en Contribuciones a las Ciencias Sociales. Disponible en www.eumed.net/rev/cccss/21/. Recuperado: 09/12/2013

Olugbode, M., Richards, R. & Biss, T., (2007), The role of information technology in achieving the organizations strategic development's goals: a case study. *Information Systems*, 32, (5), pp. 641-648 Disponible en <http://www.sciencedirect.com/science/article/pii/S0306437906000159>

Ormella Meyer, C., (2010), *¿Seguridad informática vs Seguridad de la información?*, Disponible en <http://www.criptored.upm.es/>

Páez Urdaneta I., (1992), *Gestión de la inteligencia, aprendizaje tecnológico y modernización del trabajo informacional. Retos y oportunidades*. Caracas: Universidad Simón Bolívar Disponible en <http://scielo.sld.cu/scieloOrg/php/reference.php?pid=S1024-94352004000300>

Ponjuán Dante G., (2004), *Los sistemas de información: principios y aplicaciones*. La Habana: Félix Varela

Porter Michael E. & Millar Víctor E. (1985). How information gives you competitive advantage. *Harvard Business Review*, julio issue. Recuperado el 09/12/2013 de <http://www.hbs.edu/faculty/Pages/item.aspx?num=4322>

Porter, M. (2006), *Tecnología y ventaja competitiva. Estrategia y ventaja competitiva* Ed. Deusto

Roach, S. (1987), *American's technology dilemma: a profile of the information economy*. New York: Morgan Stanley Special Economics Study.

Robbins, S.P. (2004), *Comportamiento organizacional*, Madrid: Person Educación.

Sena, L & Tenzer, S.M. (2004), *Introducción a Riesgo Informático*, FCEA Cátedra de Introducción a la Computación.

Sieber S., Valor J. & Porta V. (2006), *Los sistemas de información en la empresa actual*. Mc.Graw Hill.

Schneier, Bruce, (1994), *Applied Cryptography*, John Wiley & Sons, 2da edición

Schneier, Bruce, (2003), *Beyond Fear Thinking sensibly about security in an uncertain world*, Copernicus Books

Schneier, Bruce, (2004) *Secrets and Lies. Digital security in a networked world*, Wiley Publishing, Inc.

Solórzano, Arturo J., (2006), *Importancia de las Tecnologías de Información y Comunicación para las PYMEs*. Recuperado el 26/02/2013 de <http://www.ibcreativesolutions.com/ticpymes.html>

Stoner, J., Freeman, E. & Gilbert jr, D., (1996), *Administración*. México: Editorial Prentice Hall, 6ta edición.

Stoner, J. et al (2003). *Administración*. México: Prentice-Hall

Tanenbaum, E., (1996) *Computer Networks*. México: Prentice Hall, 3rd Ed

Villalón, A., (2002) *Seguridad de Unix y Redes Versión 2.1*. Recuperado el 27/02/2014 de <http://www.rediris.es/cert/doc/unixsec.pdf>.

Vislykh, Victor, (2007) *Examen de la gestión y administración en la organización de aviación civil internacional (OACI)*. Dependencia Común de Inspección Ginebra, Naciones Unidas Recuperado el 27/11/2014 de https://www.unjiu.org/es/corporate-information/AR%20%20PoW/A-55-34_spanish.pdf

Zhang, Yishan & Chulkov Nikolay, (2011) *Gestión de la tecnología de la información y las comunicaciones en las organizaciones del sistema de las Naciones Unidas*, Dependencia Común de Inspección, Ginebra, Naciones Unidas Recuperado el 27/11/2014 de

https://www.unjiu.org/es/reports-notes/JIU%20Products/JIU_REP_2011_9_Spanish.pdf

Direcciones de Internet.

<http://bvs.sld.cu>

<http://definicion.de/seguridad/>

<http://exa.unne.edu.ar>

<http://wso2.org>

<http://www.cubadebate.cu>

<http://www.delitosinformaticos.com>

<http://www.ecured.cu>

<http://www.espaciosoa.net>

<http://www.gacetaoficial.cu>

<http://www.google.com>

<http://www.insudeseq.com>

<http://www.ispjae.edu.cu>

<http://www.microsoft.com>

<http://www.monografias.com>

<http://www.rae.es>

<http://www.soaagenda.com>

Legislación consultada.

Acuerdo no. 6058 de 2007 Comité Ejecutivo del Consejo de Ministros Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en el País.

Decreto Ley 199/99. Sobre la Seguridad y Protección de la Información Oficial.

Resolución 127/07, Reglamento de Seguridad de las Tecnologías de Informática y Comunicaciones Ministerio de Informática y Comunicaciones

Resolución 60/11, Normas del Sistema De Control Interno. Guía de autocontrol general. Contraloría General de la República de Cuba

Anexos.

Anexo 1 Serie ISO/IEC 27000.

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Algunas de estas normas se encuentran en preparación, otras ya han sufrido actualizaciones. Incluyen:

- ISO/IEC 27000 - vocabulario estándar para el SGSI.
- ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
- ISO/IEC 27002 - *Information technology - Security techniques - Code of practice for information security management*. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
- ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
- ISO/IEC 27004 - métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de

evaluación de riesgos de Seguridad en la Información, es soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.

- ISO/IEC 27006:2007 - requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma define requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
- ISO/IEC 27007 - guía para auditar al SGSI. Se encuentra en preparación.
- ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
- ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

Anexo 2 Legislaciones más significativas en el contexto legal cubano referente a al uso de las tecnologías de la información y las comunicaciones y la información que en ellas se gestiona.

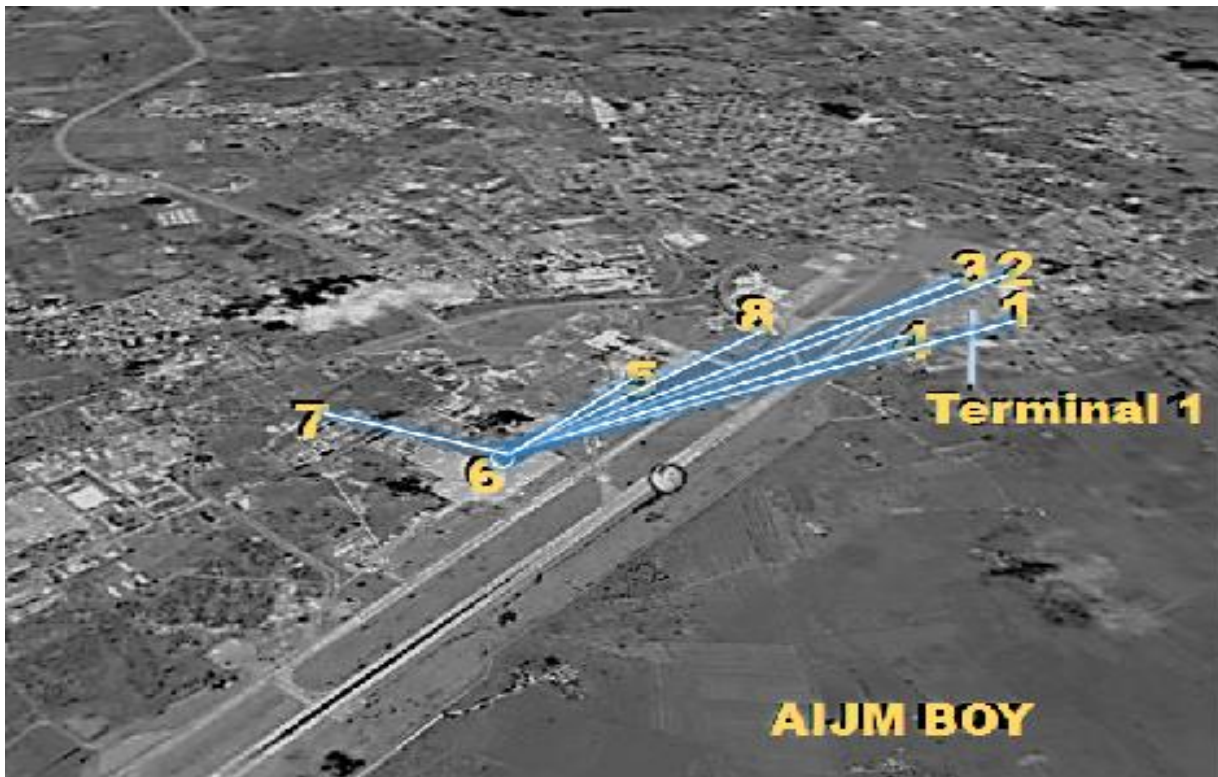
- **Acuerdo no. 84 2004**, Comité Ejecutivo del Consejo de Ministros. Organización de un programa para el paso progresivo de los sistemas de los órganos y organismos del Estado y el Gobierno hacia la plataforma de software libre
- **Acuerdo no. ____ de 2005**. Consejo de Ministros de la República de Cuba. Lineamientos para el desarrollo en Cuba del Comercio Electrónico.
- **Acuerdo no. 6058 de 2007**. Comité Ejecutivo del Consejo de Ministros. Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en el País.
- **Decreto 209/96**. Consejo de Ministros de la República de Cuba. Regulaciones para el desarrollo adecuado y armónico y en intereses de la defensa y seguridad del país, del acceso desde la República de Cuba a redes informáticas de alcance global. Designa al Ministerio del Interior responsable de dirigir, controlar y aplicar, en el marco de su competencia, la política de Seguridad Informática.
- **Decreto Ley 199/99**. Consejo de Estado. Sobre la Seguridad y Protección de la Información Oficial. El capítulo siete, es dedicado exclusivamente a la seguridad informática. Establece, entre otros aspectos, la obligación de los órganos, organismos y entidades, donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, a cumplir las medidas que se requieran para su seguridad y protección, así como elaborar, aplicar y mantener actualizados permanentemente los Planes de Seguridad Informática y de Contingencia.
- **Decreto-Ley No.469/07**. Consejo de Estado. Actas de Compromiso de los trabajadores con sus deberes y obligaciones como usuarios de la Red
- **Resolución 6/1996**. Ministerio del Interior. Pone en vigor el Reglamento sobre la Seguridad informática, dado a cumplimentar las medidas establecidas para la protección y seguridad del Secreto Estatal y la Protección Física.

- **Resolución 204/1996.** Ministerio de la Industria Sidero Mecánica y Electrónica. Reglamento sobre la protección y seguridad técnica de los Sistemas Informáticos.
- **Resolución 56/1999.** Ministerio de Cultura. Establece que toda publicación seriada cubana, para circular o difundirse por Internet, deberá constar con la aprobación específica del Registro Nacional de Publicaciones Seriadas
- **Resolución 22/2000.** Ministerio de la Informática y las Comunicaciones. Metodología para el funcionamiento de redes privadas de datos en Cuba.
- **Resolución 2620/2000.** Oficina Cubana de la Propiedad Industrial del Ministerio de Ciencia, Tecnología y Medio Ambiente. Establece la búsqueda, en las bases de datos, de marcas, nombres comerciales, emblemas empresariales, rótulos de establecimiento, lemas comerciales y denominaciones de origen, de aquellas denominaciones que constituyan o integren estos signos distintivos y que resulten idénticas a las denominaciones cuyo registro, como nombre de dominio, haya sido solicitado
- **Resolución 90/2000.** Ministerio de la Informática y las Comunicaciones. Reglamentar el uso de un punto para la interconexión nacional.
- **Resolución 124/2000.** Ministerio de la Informática y las Comunicaciones. Registro de Direcciones IP de la República de Cuba.
- **Resolución 1/2000.** Ministerio del Interior. Establece el Reglamento sobre la seguridad y protección de la información oficial y el modo en que se aplicarán las normas de seguridad establecidas en el Decreto Ley 199.
- **Resolución 185/2001.** Ministerio de la Informática y las Comunicaciones. Regula lo relativo al funcionamiento de los proveedores de servicios de Internet en Cuba.
- **Resolución 188/2001.** Ministerio de la Informática y las Comunicaciones. Aprueba y pone en vigor la Metodología para el Acceso de las Entidades Cubanas a Internet o a otras Redes de Datos Externas.
- **Resolución 13/2003.** Centro Nacional de Derecho de Autor del Ministerio de Cultura. Sobre el registro de los derechos autorales sobre programas de computación y bases de datos y la manera en que se lleva a cabo dicho registro.
- **Resolución 39/2002.** Ministerio de la Informática y las Comunicaciones. Políticas de Seguridad Informática del Ministerio de la Informática y las Comunicaciones

- **Resolución 119/2002.** Empresa CITMATEL del Ministerio de Ciencia, Tecnología y Medio Ambiente. Regula el procedimiento de administración de los nombres de dominio .cu.
- **Resolución 65/2003.** Ministerio de la Informática y las Comunicaciones. Parámetros para la inscripción de cualquier red de datos establecida en el territorio nacional de la República de Cuba.
- **Resolución 92/2003.** Ministerio de la Informática y las Comunicaciones. Regula la creación, en los sitios web cubanos que ofrecen servicio de correo electrónico, de cuentas (*webmail*) de forma automática para personas naturales o jurídicas que no se encuentren debidamente autorizadas.
- **Resolución 93/2003.** Ministerio de la Informática y las Comunicaciones. Regula la ubicación en servidores en Cuba de los sitios cubanos bajo el nombre de dominio .cu.
- **Resolución 180/2003.** Ministerio de la Informática y las Comunicaciones. Normas que restringen el acceso a Internet a personas no autorizadas.
- **Resolución 85/2004.** Ministerio de la Informática y las Comunicaciones. Regula las áreas para brindar servicios de navegación y correo electrónico a personas naturales desde hoteles, oficinas de correo u otros establecimientos autorizados.
- **Resolución 127/2007.** Ministerio de Informática y Comunicaciones. Reglamento de Seguridad de las Tecnologías de Informática y Comunicaciones.
- **Resolución Conjunta 1/1999.** Ministerio de Comercio Exterior y Ministerio de la Industria Sidero Mecánica y la Electrónica. Creación de la Comisión Nacional para el Comercio Electrónico
- **Resolución Conjunta 1/1999.** Ministerio de Cultura y Ministerio de la Industria Sidero Mecánica y la Electrónica. Pone en vigor el Reglamento para la protección de programas de computación, sus versiones sucesivas y programas derivados, con independencia de la forma de creación y el soporte que los contenga.
- **Resolución Conjunta __/2004.** Ministerio de la Informática y las Comunicaciones y Ministerio de Finanzas y Precios. Se establecen los requisitos que deben cumplir los Sistemas Contables-financieros soportados sobre las tecnologías de la información para ser utilizados en las empresas del país.

Anexo 3 Ubicación geográfica de las entidades que componen Cubana de Aviación S.A.

Ubicación de las áreas de Cubana de Aviación S.A. en el Aeropuerto Internacional José Martí en Boyeros.

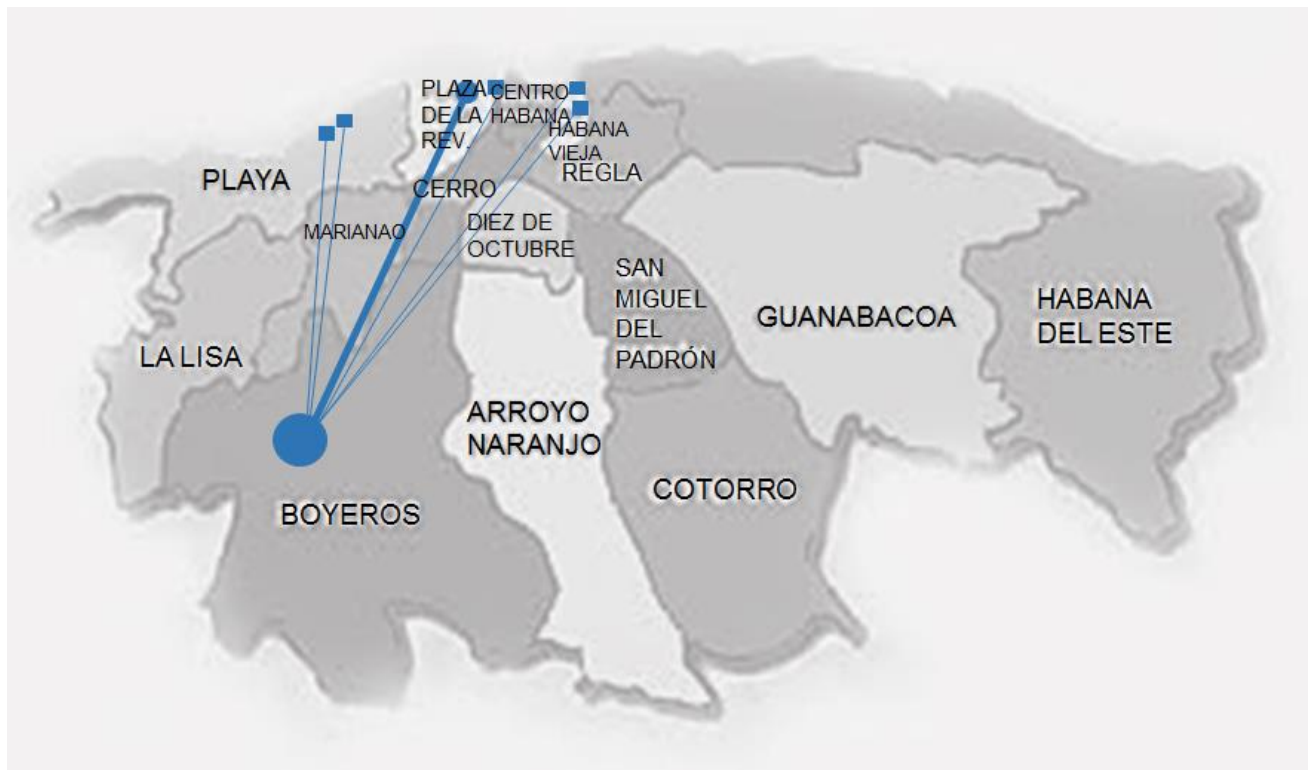


Áreas:

1. Terminal número 1:
 - Dir. Economía
 - Dir. Contabilidad
 - Dirección TIC
 - NCSI
 - Dir. Seguridad y Calidad Vuelos
 - Dir. Seguridad y protección a Vuelos.
2. Vicepresidencia de Operaciones (OPE)
3. Recursos Humanos (RRHH)
4. Venta a Bordo y Carga Nacional
5. Terminal número 3:
 - Línea Aérea
 - Lost & Found
 - Centro Control Operacional

6. Dirección General de la empresa, Direcciones y Departamentos independientes y Talleres Aeronáuticos de Reparación
7. Almacenes
8. Terminal número 4 o Aerovaradero
 - Dirección de Carga
 - Carga Internacional

Ubicación de las áreas de Cubana de Aviación S.A. en el territorio de la provincia de La Habana.



Áreas:

1. AIJM
2. Plaza de la Revolución:
 - NASI
 - Unidad Ventas Vuelos Internacionales
 - Unidad Ventas Vuelos Nacionales
3. Puntos de Venta:
 - 5ta y 110
 - Centro de Negocios de Miramar
 - Enridan (frente al Capitolio Nacional)
 - Lonja del Comercio

Ubicación de las áreas de Cubana de Aviación S.A. en el territorio nacional.



Áreas:

1. La Habana
2. Isla de la Juventud
3. Matanzas
 - Cayo Largo del Sur
 - Cienfuegos
 - Santa Clara
4. Camagüey
 - Ciego de Ávila
 - Cayo Coco
5. Las Tunas
 - Bayamo
 - Manzanillo
6. Holguín
 - Moa
7. Santiago de Cuba
 - Guantánamo
 - Baracoa

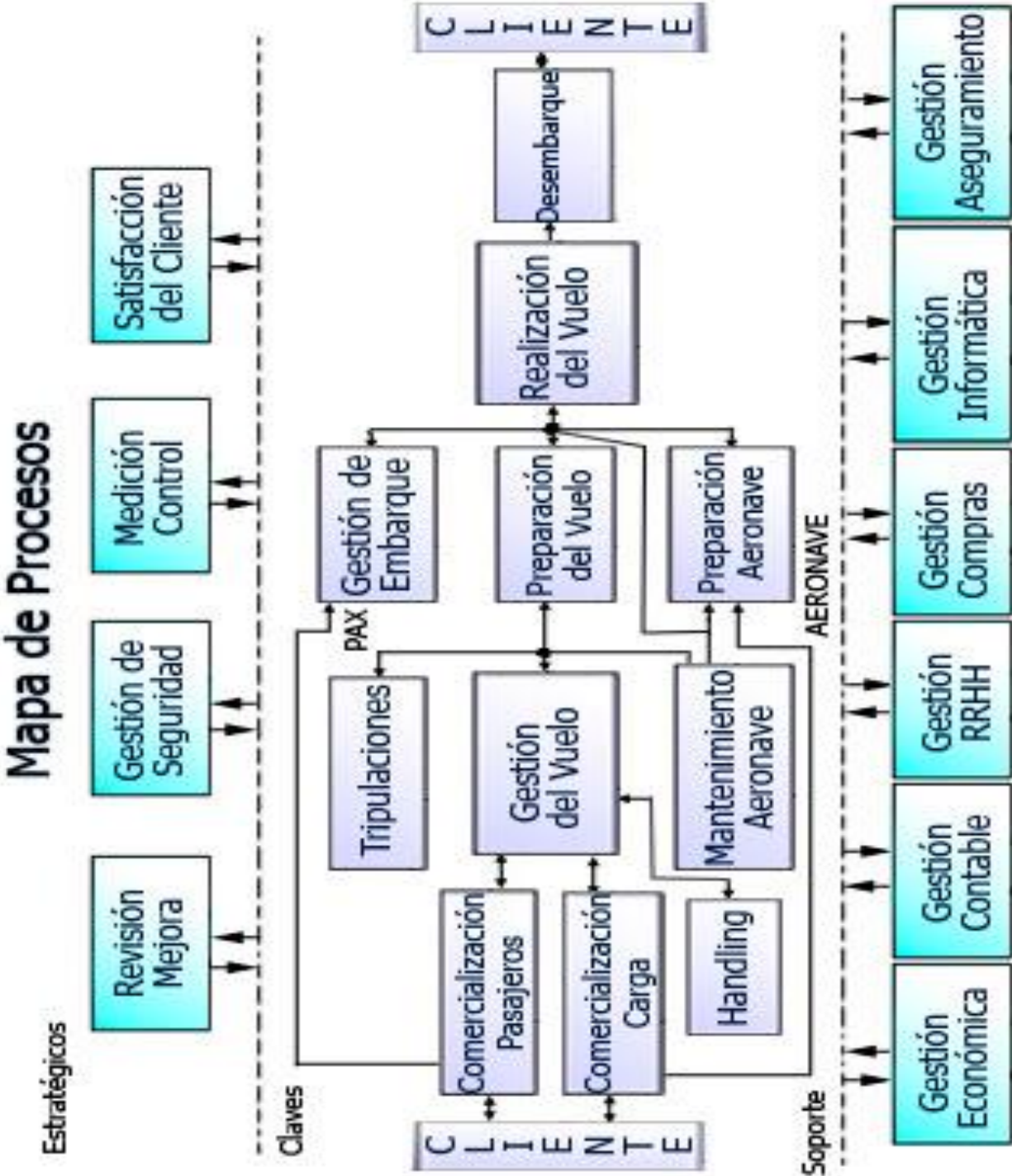
Ubicación de las áreas de Cubana de Aviación S.A. en el mundo.



Áreas:

- | | |
|---------------|----------------|
| 1. Montreal | 12. Venezuela |
| 2. Toronto | 13. Argentina |
| 3. México DF | 14. Brasil |
| 4. Cancún | 15. Dominicana |
| 5. Belice | 16. Haití |
| 6. Honduras | 17. Martinica |
| 7. Nicaragua | 18. Bahamas |
| 8. Costa Rica | 19. España |
| 9. Panamá | 20. Francia |
| 10. Colombia | 21. Italia |
| 11. Ecuador | 22. Rusia |

Anexo 4 Mapa de procesos CU



Anexo 5 Análisis de la situación actual (agosto 2015) en las tecnologías de la información y las comunicaciones en Cubana de Aviación S.A. (Matriz DAFO)

	FACTORES EXTERNOS	
	OPORTUNIDADES	AMENAZAS
FACTORES INTERNOS	<ol style="list-style-type: none"> Existencia de Lineamientos Estratégicos para la Informatización de la Sociedad Cubana aprobados por el CECM. Existencia de un Ministerio de Comunicaciones, así como de una Comisión Nacional de Informática a la cual pertenecemos. Atención metodológica de una agencia estatal especializada, la OSRI, en materia de Seguridad de las Tecnologías de la Información Favorables y estables relaciones con empresas nacionales y extranjeras suministradoras de Tecnologías de Información y Servicios Informáticos. Aplicación creciente de la informática en la aviación al punto de comenzar a constituirse en una exigencia de los organismos internacionales Existencia de la Universidad de las Ciencias Informáticas UCI y de especialidades 	<ol style="list-style-type: none"> Bloqueo económico y financiero de Estados Unidos al país. Ritmo creciente de los cambios en las tecnologías de información a nivel internacional. Ofertas más atractivas a los especialistas informáticos por entidades nacionales y extranjeras. Ataques a nuestras redes de transmisión de datos con vistas a dañarlas, a obtener, modificar o destruir información sensible, así como a dañar la imagen internacional de la aeronáutica civil cubana. Uso de software no adquirido lícitamente que puede conllevar a la aplicación de sanciones o quedar comprometida la actualización de los mismos con el consiguiente incremento de los riesgos. Averías en la Red por fluctuaciones de corriente y posibles influencias de descargas eléctricas. Paralización de los servicios suministrados

	<p>informáticas en el resto de las Universidades del Sistema de Educación Superior</p> <p>7. Incremento de la matrícula en los Politécnicos de Informática, así como la remodelación y mejoras de condiciones para el estudio en cada uno de ellos.</p> <p>8. Acceso a INTERNET que favorece el incremento de la calificación autodidacta del personal de informática en las más novedosas técnicas y equipamiento existentes.</p> <p>9. Existencia de un reglamento actualizado para la Seguridad de las Tecnologías de la Información a nivel gubernamental, materializado en la Resolución No. 127/2007 del M.I.C.</p> <p>10. Existencia, a nivel internacional, de documentos regulatorios sobre el uso de las TICs y su seguridad.</p> <p>11. Existencia de modelos para la organización del gobierno de las tecnologías orientados al control interno.</p> <p>12. Existencia de entidades certificadas en el país para el desarrollo de sistemas informáticos.</p>	<p>por proveedores extranjeros como SITA, AMADEUS e IBERIA.</p> <p>8. Atención en materia de las TICs en las Unidades en el exterior dada por personal del país contratado, sin un criterio definido y aprobado por la Dirección de Informática y Comunicaciones para su selección. En los contratos firmados con estas terceras personas no aparecen explícitamente acuerdos referentes al cumplimiento del SGSI establecido por la organización.</p> <p>9. Pobre utilización de vías seguras para la transmisión de información desde las Unidades en el exterior.</p> <p>10. Poca atención a las tecnologías instaladas en las unidades en el exterior. Proveedores de servicios del país.</p> <p>11. Fusión de IBERIA con British Airways.</p>
--	--	--

	13. Existencia de entidades certificadas en el país para el desarrollo de sistemas de aseguramiento y soporte (seguridad física, aterramiento).	
FORTALEZAS		
1. Existencia de una Dirección Rectora de la Informática y la Automatización en la CACSA, así como de un Consejo de esta especialidad que funciona establemente. 2. Existencia de una entidad informática organizativa en el nivel central, así como de especialistas aislados en todas sus unidades nacionales que poseen medios y sistemas de computación. 3. Existencia de especialistas en informática y automatización con años de experiencia dentro de la institución. Experiencia acumulada. 4. Existencia de una red de transmisión de datos propia de la aeronáutica civil con acceso internacional, incluido el acceso a INTERNET, así como un amplio empleo del correo electrónico y la mensajería por todas las dependencias. Esta red brinda además otros servicios de valor agregado como son el	1. <i>Evaluar nuevas herramientas para el desarrollo de aplicaciones propias. Elección de las mismas.</i> 2. <i>Definir programa de capacitación en base a las herramientas seleccionadas.</i> 3. <i>Cotización de las herramientas y defensa de su adquisición.</i> 4. <i>Elaborar y defender presupuestos de inversiones y gastos que garanticen la modernización paulatina de las tecnologías.</i> 5. <i>Actualización de los sistemas propios según las nuevas herramientas implementadas. Desarrollo de otros nuevos.</i> 6. <i>Concertar acuerdos con entidades desarrolladoras de reconocidos resultados.</i>	1. <i>Solicitar sea incluido en el contrato de trabajo el cumplimiento de las Políticas de Seguridad y del Código de Ética para el uso de las tecnologías.</i> 2. <i>Solicitar a las áreas demandantes de sistemas, la documentación establecida para el desarrollo de los mismos y de los procesos a automatizar.</i> 3. <i>Estimar los costos de nuevos desarrollos de conjunto con el área demandante y teniendo en cuenta todos los momentos del proceso (capacitación de los desarrolladores, capacitación de los usuarios, contratación de terceros, implementación, pruebas y puesta en explotación), para tomar la decisión.</i> 4. <i>Elaborar Plan de Capacitación a los usuarios de los sistemas según sean</i>

<p>acceso remoto, el uso del correo propio desde cualquier país, etc.</p> <p>5. Existencia generalizada de medios técnicos de computación y redes locales en todas las unidades de la empresa.</p> <p>6. Experiencia en el desarrollo y explotación de sistemas automatizados propios o adquiridos para el procesamiento de la información.</p> <p>7. Aceptable nivel de introducción de herramientas de software para la protección de las redes, sistemas y equipos de computación.</p> <p>8. Existencia de un portal en la Intranet, al cual tienen acceso todos los usuarios de la aviación para publicar y obtener información.</p> <p>9. Experiencia en la evaluación y prueba de nuevos software específicos que garantiza que los mismos cumplen los requerimientos previos establecidos por la compañía y organismos e instituciones nacionales e internacionales.</p> <p>10. Existencia de una incipiente cultura de la seguridad de las tecnologías de la información en la organización y profesionalidad de los responsables de la misma.</p>		<p><i>implementados estos.</i></p> <p>5. <i>Solicitar la capacitación del personal en sistemas de escritorio (Office).</i></p> <p>6. <i>Comprobar conocimientos, en el momento en que se opta por la plaza, del manejo y uso de las tecnologías de la información.</i></p> <p>7. <i>Desarrollar o adquirir aplicaciones que permitan un monitoreo más eficiente del tráfico de red (intranet, internet).</i></p> <p>8. <i>Seguimiento constante al cumplimiento de los presupuestos aprobados.</i></p> <p>9. <i>Evaluación sistemática de la seguridad de las tecnologías y la información y actualización de los planes de mejora.</i></p> <p>10. <i>Participación en la determinación de los riesgos y en la confección de los PSI de las áreas.</i></p> <p>11. <i>Participación en la determinación de los riesgos y en la confección de los PSI de las Unidades en el exterior. Exigencia del cumplimiento de las Políticas definidas al respecto.</i></p>
--	--	--

<p>11. Existencia de una política de empresa para el uso de los recursos informáticos que se concreta en procedimientos y reglamentos definidos para cada uno.</p> <p>12. Existe definido el conjunto de Políticas para el Sistema de Gestión de Seguridad de la Información (SGSI) y el Sistema de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC).</p>		<p><i>12. Contratar la instalación, revisión y certificación de los sistemas de aterramiento de nodos y locales tecnológicos.</i></p>
DEBILIDADES	<p><i>1. Contratación de desarrolladores.</i></p> <p><i>2. Utilizar herramientas modernas que faciliten la realización de los desarrollos.</i></p> <p><i>3. Definir la estructura hardware necesaria y solicitar su adquisición.</i></p> <p><i>4. Elaborar planes de capacitación en nuevas tecnologías adquiridas.</i></p> <p><i>5. Elaborar planes de comunicación (web de la intranet, seminarios, talleres, boletines) de objetivos, noticias, nuevos sistemas, estado del arte de las tecnologías.</i></p> <p><i>6. Elaborar procedimientos y formularios de pruebas internas y con el usuario.</i></p> <p><i>7. Solicitar a la Dirección de Capital Humano que</i></p>	<p><i>1. Adoptar proveedores seguros.</i></p> <p><i>2. Cumplir los Planes de Mantenimiento de los MTC en porcentos elevados.</i></p> <p><i>3. Mantener vigilancia constante sobre los accesos a la red y la información que por ella se mueve, los servicios y su utilización adecuada y oportuna.</i></p> <p><i>4. Migración paulatina, según las posibilidades, a aplicaciones de código abierto para evitar el uso de licencias de SO y aplicaciones.</i></p> <p><i>5. Priorizar en los planes de presupuesto el completamiento de los sistemas de</i></p>
<p>1. No está considerado como un objetivo estratégico de la empresa el desarrollo de las tecnologías.</p> <p>2. Insuficiente fuerza de trabajo calificada para cumplir con las funciones asignadas, especialmente en las actividades de Ingeniería y Redes y de Servicios Técnicos (actividad de soporte).</p> <p>3. Insuficiente preparación de especialista y técnicos por carencia de una capacitación, no autodidacta, actualizada y permanente en temas específicos en función de los cambios acelerados del entorno (desarrollo de software, nuevos sistemas, aplicaciones, seguridad informática, en especial análisis forense de incidentes y eventos, administración de redes, comunicaciones, entre</p>		

<p>otros).</p> <p>4. Presupuestos de inversiones y gastos insuficientes para garantizar la actualización sistemática de las tecnologías.</p> <p>5. Bajo conocimiento de los usuarios sobre el uso de las nuevas tecnologías de información para garantizar un amplio y eficiente empleo de INTERNET y de la INTRANET.</p> <p>6. Insuficiente capacitación a los usuarios de las tecnologías.</p> <p>7. Insuficientes condiciones de trabajo y de transporte de los especialistas para el desarrollo de su labor tanto en las filiales como en el Nivel Central.</p> <p>8. Baja velocidad de los enlaces de la red WAN.</p> <p>9. Excesiva cantidad de Planes de Seguridad Informática, dado por la cantidad de áreas administrativas dispersas en el territorio que ocupa la empresa.</p> <p>10. Desconocimiento por los usuarios de los riesgos de violación de la Seguridad Informática. Subvaloración de su importancia. Falta de compromiso.</p> <p>11. Insatisfactorio aprovechamiento de los recursos de red al ser utilizados por los usuarios en actividades que no se corresponden con el Objeto Social de la empresa y del contenido de sus funciones.</p> <p>12. Locales inadecuados para el desarrollo del</p>	<p><i>cada área presente un Plan de Capacitación en sistemas instalados y aplicaciones de escritorio. Coordinar su realización.</i></p> <p><i>8. Elaborar Plan de Contingencias de la Dirección de Informática y Comunicaciones.</i></p> <p><i>9. Reestructuración de la Dirección de Informática y Comunicaciones teniendo en cuenta las observaciones e indicaciones de auditorías, inspecciones y controles.</i></p> <p><i>10. Actualizar la documentación del cableado estructurado, incluyendo el realizado en nuevos locales.</i></p> <p><i>11. Asumir la dirección de trabajos de diplomas de universidades con temas de interés y que solucionen problemas identificados.</i></p> <p><i>12. Asumir la recepción de estudiantes de los Institutos Tecnológicos en sus periodos de prácticas productivas para apoyar el trabajo de especialistas y técnicos.</i></p> <p><i>13. Trabajar en la documentación necesaria para la confección de un PSI único para toda la</i></p>	<p><i>aterramiento pendientes.</i></p> <p><i>6. Incluir en los contratos con proveedores extranjeros en que no existan, cláusulas que protejan ante problemas de suministro de servicios.</i></p> <p><i>7. Exigir el cumplimiento de las Políticas para el SGSI y la STIC en las Unidades en el exterior, incluyendo en los contratos de trabajo y servicios lo pertinente. Designar un Especialista de la DTIC por Unidad para su vigilancia.</i></p> <p><i>8. Obligar al uso de las vías seguras de intercambio de información con el exterior. Notificar las violaciones e informar en el Consejo de Dirección.</i></p> <p><i>9. Continuar proponiendo al Consejo de Dirección se asuma lo referente al desarrollo de las TICs como objetivo estratégico de la organización. Continuar asumiéndolo como objetivo propio de la DTIC con alcance a toda la empresa.</i></p> <p><i>10. Organizar capacitación interna, tanto técnica como para usuarios,</i></p>
--	---	--

<p>trabajo de la especialidad en la empresa y unidades nacionales.</p> <p>13. Desfase entre la rápida modernización de las nuevas tecnologías de información (equipos y sistemas) y su introducción en el aseguramiento de los procesos de la empresa, así como en la actualización en su empleo por los especialistas y técnicos en informática.</p> <p>14. No utilización de los procesos de certificación de los especialistas en temas de informática.</p> <p>15. Insuficiente uso y disponibilidad de software para la automatización del monitoreo y control de los recursos informáticos con vistas a la prevención de los incidentes de seguridad informática y robo de componentes, en lugar de su análisis forense.</p> <p>16. Insuficientes recursos destinados a la salvaguarda de la información empresarial y las establecidas como obligatorias por las regulaciones gubernamentales.</p> <p>17. La existencia de 22 gerencias en 20 países, no permite el adecuado seguimiento de los planes de seguridad informática de estas gerencias, no siendo analizadas las vulnerabilidades y los riesgos con la frecuencia necesaria.</p> <p>18. Insuficiente aplicación de las políticas empresariales de seguridad informática en las unidades del exterior</p>	<p><i>empresa, de manera que sea posible enfrentar las amenazas, vulnerabilidades y riesgos de forma ordenada y con prioridades bien establecidas</i></p>	<p><i>aprovechando los especialistas y técnicos de mejor preparación profesional, como forma de suplir la carencia de capacitación con terceros. Hacia lo interno de la DTIC, programar el espacio Consejo Técnico, el último jueves de cada mes para análisis, debate y preparación de los especialistas y técnicos.</i></p> <p><i>11. Continuar solicitando presupuestos, debidamente justificados, para la modernización y actualización de las TICs.</i></p> <p><i>12. Mejorar las condiciones de trabajo a partir de las fuerzas propias de la DTIC y la creatividad y los aportes del colectivo.</i></p> <p><i>13. Utilizar diferentes vías de comunicación para dar a conocer lo relacionado con la STIC y la necesidad de su cumplimiento.</i></p> <p><i>14. Priorizar la adquisición de tecnologías que garanticen mayores velocidad en la red, la salvaguarda de la información y el monitoreo del uso de</i></p>
--	---	---

<p>por razones técnicas y administrativas.</p> <p>19. Explotación de diferentes versiones de una misma aplicación o sistemas, no distribuidos por la Red Corporativa.</p> <p>20. Indisciplinas en el uso de los recursos informáticos como la comunicación de los accesos y contraseñas propios a otras personas y actividades no autorizadas en las aplicaciones.</p> <p>21. Uso inapropiado de los canales de comunicación telefónica.</p> <p>22. Existencia de 43 PSI en la empresa, resultado de 47 análisis de riesgos. No se ve el PSI como instrumento de dirección,</p> <p>23. Falta de alternativas de solución para el caso de producirse suspensiones de los servicios por proveedores extranjeros como SITA, AMADEUS e IBERIA.</p> <p>24. No se especifican los conocimientos necesarios sobre las TICs para ocupar plazas específicas dentro de la organización.</p> <p>25. Los puestos de trabajo no tienen definidos los recursos mínimos necesarios de TICs para el cumplimiento de sus funciones.</p> <p>26. Ausencia de una adecuada comprensión en la conciencia de la organización de la necesidad del cumplimiento de las normas de la Seguridad de la Información.</p> <p>27. No poseer las condiciones técnicas y de</p>		<p><i>los medios.</i></p> <p><i>15. Estandarización de los SO, SW y aplicaciones en todas las áreas de la entidad (nacionales y exterior).</i></p> <p><i>16. Revisar y redefinir los recursos necesarios para cada puesto de trabajo y las competencias digitales, o habilidades informáticas, que se requieren para ocupar los mismos.</i></p> <p><i>17. Completar la documentación de los sistemas propios. Certificar los que cumplan con los requisitos que se exigen.</i></p>
---	--	--

<p>seguridad necesarias para obtener certificación para la navegación por Internet, lo que obliga a depender de la CACSA para acceder a estos servicios.</p> <p>28. Deficiente documentación de sistemas propios.</p> <p>29. Falta de estandarización en sistemas y servicios.</p> <p>30. Carencia o deficientes sistemas de seguridad ante descargas eléctricas en nodos y locales tecnológicos.</p> <p>31. Carencia o deficiente climatización en locales tecnológicos.</p>		
---	--	--

Estrategias FO ofensivas (fortalezas vs oportunidades)	
O1	Evaluar nuevas herramientas para el desarrollo de aplicaciones propias. Elección de las mismas.
O2	Definir programa de capacitación en base a las herramientas seleccionadas.
O3	Cotización de las herramientas y defensa de su adquisición.
O4	Elaborar y defender presupuestos de inversiones y gastos que garanticen la modernización paulatina de las tecnologías.
O5	Actualización de los sistemas propios según las nuevas herramientas implementadas. Desarrollo de otros nuevos.
O6	Concertar acuerdos con entidades desarrolladoras de reconocidos resultados.
Estrategias FA defensivas (fortalezas vs amenazas)	
D1	Solicitar sea incluido en el contrato de trabajo el cumplimiento de las Políticas de Seguridad y del Código de Ética para el uso de las tecnologías.
D2	Solicitar a las áreas demandantes de sistemas, la documentación establecida para el desarrollo de los mismos y de los procesos a automatizar.
D3	Estimar los costos de nuevos desarrollos de conjunto con el área demandante y teniendo en cuenta todos los momentos del proceso (capacitación de los desarrolladores, capacitación de los usuarios, contratación de terceros, implementación, pruebas y puesta en explotación), para tomar la decisión.
D4	Elaborar Plan de Capacitación a los usuarios de los sistemas según sean implementados estos.
D5	Solicitar la capacitación del personal en sistemas de escritorio (MS Office).

D6	Comprobar conocimientos, en el momento en que se opta por la plaza, del manejo y uso de las tecnologías de la información.
D7	Desarrollar o adquirir aplicaciones que permitan un monitoreo más eficiente del tráfico de red (intranet, internet).
D8	Seguimiento constante al cumplimiento de los presupuestos aprobados.
D9	Evaluación sistemática de la seguridad de las tecnologías y la información y actualización de los planes de mejora.
D10	Participación en la determinación de los riesgos y en la confección de los PSI de las áreas.
D11	Participación en la determinación de los riesgos y en la confección de los PSI de las Unidades en el exterior. Exigencia del cumplimiento de las Políticas definidas al respecto.
D12	Contratar la instalación, revisión y certificación de los sistemas de aterramiento de nodos y locales tecnológicos.
Estrategias DO reorientación (debilidades vs oportunidades)	
R1	Contratación de desarrolladores.
R2	Utilizar herramientas modernas que faciliten la realización de los desarrollos.
R3	Definir la estructura hardware necesaria y solicitar su adquisición.
R4	Elaborar planes de capacitación en nuevas tecnologías adquiridas.
R5	Elaborar planes de comunicación (web, seminarios, boletines) de objetivos, noticias, nuevos sistemas, estado del arte de las tecnologías.
R6	Elaborar procedimientos y formularios de pruebas internas y con el usuario.
R7	Solicitar a la DCH que cada área presente un Plan de Capacitación en sistemas instalados y aplicaciones de escritorio. Coordinar su realización.
R8	Elaborar Plan de Contingencias de la Dirección de Informática y Comunicaciones.
R9	Reestructuración de la DTIC teniendo en cuenta las observaciones e indicaciones de auditorías, inspecciones y controles.
R10	Actualizar la documentación del cableado estructurado, incluyendo el realizado en nuevos locales.
R11	Asumir la dirección de trabajos de diplomas de universidades con temas de interés y que solucionen problemas identificados.
R12	Asumir la recepción de estudiantes de los IPI en sus periodos de prácticas productivas para apoyar el trabajo de especialistas y técnicos.
R13	Trabajar en la documentación necesaria para la confección de un PSI único para toda la empresa, de manera que sea posible enfrentar las amenazas, vulnerabilidades y riesgos de forma ordenada y con prioridades bien establecidas

Estrategias DA supervivencia (debilidades vs amenazas)	
S1	Adoptar proveedores seguros. Buscar alternativas para servicios como los prestados por SITA, AMADEUS e IBERIA.
S2	Cumplir los Planes de Mantenimiento de los MTC en porcentos elevados.
S3	Mantener vigilancia constante sobre los accesos a la red y la información que por ella se mueve, los servicios y su utilización adecuada y oportuna.
S4	Migración paulatina, según las posibilidades, a aplicaciones de código abierto para evitar el uso de licencias de SO y aplicaciones.
S5	Priorizar en los planes de presupuesto el completamiento de los sistemas de aterramiento pendientes.
S6	Incluir en los contratos con proveedores extranjeros en que no existan, cláusulas que protejan ante problemas de suministro de servicios.
S7	Exigir el cumplimiento de las Políticas para el SGSI y la STIC en las Unidades en el exterior, incluyendo en los contratos de trabajo y servicios lo pertinente. Designar un Especialista de la DTIC por Unidad para su vigilancia.
S8	Obligar al uso de las vías seguras de intercambio de información con el exterior. Notificar las violaciones e informar en el Consejo de Dirección.
S9	Continuar proponiendo al Consejo de Dirección se asuma lo referente al desarrollo de las TICs como objetivo estratégico de la organización. Continuar asumiéndolo como objetivo propio de la DTIC con alcance a toda la empresa.
S10	Organizar capacitación interna, tanto técnica como para usuarios, aprovechando los especialistas y técnicos de mejor preparación profesional, como forma de suplir la carencia de capacitación con terceros. Hacia lo interno de la DTIC, programar el espacio Consejo Técnico, el último jueves de cada mes para análisis, debate y preparación de los especialistas y técnicos.
S11	Continuar solicitando presupuestos, debidamente justificados, para la modernización y actualización de las TICs.
S12	Mejorar las condiciones de trabajo a partir de las fuerzas propias de la DTIC y la creatividad y los aportes del colectivo.
S13	Utilizar diferentes vías de comunicación para dar a conocer lo relacionado con la STIC y la necesidad de su cumplimiento.
S14	Priorizar la adquisición de tecnologías que garanticen mayores velocidad en la red, la salvaguarda de la información y el monitoreo del uso de los medios.
S15	Estandarización de los SO, software y aplicaciones en todas las áreas de la entidad (nacionales y en el exterior).
S16	Revisar y redefinir los recursos necesarios para cada puesto de trabajo y las competencias digitales, o habilidades informáticas, que se requieren para ocupar los mismos.
S17	Completar la documentación de los sistemas propios. Certificar los que cumplan con los requisitos que se exigen.

Anexo 6 Relación de dependencias administrativas pertenecientes a Cubana de Aviación S.A. en el territorio de la República de Cuba y en el exterior

CONCEPTOS DE LOCALIZACIÓN GEOGRÁFICOS:

Región: Ubicación asociada a provincia en este caso (Ej.: HABANA, VARADERO)

Zona: Ubicación asociada a municipio (Ej.: HAV - apto. Boyeros, RAM – Rampa)

Área: Ubicación asociada localidad dentro de la zona (Ej.: T1 - terminal 1, T3-terminal 3, TARHAV, zona de carga de Aerovaradero)

Planta: referencia al nivel o altura en una edificación, nivel de superficie se considera Planta Baja

Edificación: estructura civil como unidad

LEYENDA:

S-TIC: Seguridad Informática o Seguridad de las Tecnologías de la Información y las Comunicaciones.

PSI: Documento formal del Plan de Seguridad Informática que debe reflejar el Sistema de Seguridad Informática implementado que es el elemento esencial.

Numeración de referencia del PSI:

1: PSI General de toda la empresa, ya que en un elevado por ciento (>97%) las Políticas de Seguridad de los Sistemas y Servicios están centralizadas y controlado su cumplimiento en el Nivel Central de la Dirección de Tecnologías de la Información y las Comunicaciones.

n: Indica PSI Específico al área en cuestión, que refleja aquellos aspectos de seguridad informática pertenecientes a dicha área.

Un área puede ser una Entidad Administrativa o un Grupo de Entidades Administrativas que comparten los mismos aspectos de la seguridad informática.

Estas especificidades provienen esencialmente de la diferencia de las áreas respecto de las vulnerabilidades y por ende del Análisis de Riesgos Informáticos, las que pueden provenir de aspectos tales como: localización geográfica, uso de servicios informáticos específicos, uso de aplicaciones informáticas específicas, características del servicio de energía eléctrica, características del personal que emplea las Tecnologías de la Información y las Comunicaciones y otras.

En el territorio de la República de Cuba

ID		REGION	ZONA	AREA	EDIF.	NIVEL	PSI	ANAL. RIESGOS
01	NCSI (Nodo Central de Servicios Informáticos)	HABANA	AIJM	T1	T1	1	1.0	1
02	DIRECCION DE TECNOLOGIAS DE INFOCOMUNICACIONES	HABANA	AIJM	T1	T1	1	1.0	1
03	DIRECCION ECONOMIA	HABANA	AIJM	T1	T1	1	1.0	1
04	DIRECCION CONTABILIDAD	HABANA	AIJM	T1	T1	1	1.0	1
	DIRECCIÓN DE SEGURIDAD DE VUELOS	HABANA	AIJM	T1	T1	1	1.2	2
	INVERSIONES,	HABANA	AIJM	T1	T1	1	1.3	3
	CAJA CENTRAL,	HABANA	AIJM	T1	T1	1	1.3	3
	DIRECCIÓN ASEGURAMIENTO	HABANA	AIJM	T1	T1	1	1.3	3
	- UNIDAD ADMINISTRATIVA BÁSICA	HABANA	AIJM	T1	T1	1	1.3	3
	- ATM	HABANA	AIJM	T1	T1	1	1.3	3
	COMBUSTIBLE	HABANA	AIJM	T1	T1	1	1.3	3
	LÍNEA AÉREA - ATENCIÓN A PASAJEROS	HABANA	AIJM	T1	T1	1	1.4	4
	LOST AND FOUND - T1	HABANA	AIJM	T1	T1	1	1.4	4
	CONTABILIDAD LÍNEA AÉREA	HABANA	AIJM	T1	T1	1.5	1.3	3
	TRÁMITES Y PROTOCOLO	HABANA	AIJM	T1	T1	1.5	1.3	3
	DIRECCION DE SEGURIDAD Y PROTECCIÓN A VUELOS	HABANA	AIJM	T1	T1	3	1.22	26
	OFICINA DEL JEFE DE LÍNEA AÉREA EN LA TERMINAL NO. 1	HABANA	AIJM	T1	T1	2	1.4	4
	DIRECCIÓN COMERCIAL	HABANA	AIJM	T1	T1	2	1.4	4
	○ SEGUNDA DIRECCION GENERAL ADJUNTA	HABANA	AIJM	T1	T1	2	1.4	4
	○ DPTOS. DIR. COMERCIAL	HABANA	AIJM	T1	T1	2	1.4	4
	AULAS DE TRIPULANTES	HABANA	AIJM	PLAZA F.A.	PLAZA F.A.	1	1.5	5
	DIRECCIÓN DE OPERACIONES	HABANA	AIJM	T1	BUNKER	1-2	1.5	6
	- PLANTA BAJA	HABANA	AIJM	T1	BUNKER	1	1.5	6
	- PLANTA ALTA	HABANA	AIJM	T1	BUNKER	2	1.5	6
	DIRECCION DE RECURSOS HUMANOS	HABANA	AIJM	T1	BUNKERCITO	1-2	1.6	7
	- PLANTA BAJA	HABANA	AIJM	T1	BUNKERCITO	1	1.6	7
	- PLANTA ALTA	HABANA	AIJM	T1	BUNKERCITO	2	1.6	7
	CENTRO CONTROL OPERACIONAL (CCO o OX o DESPACHO VUELOS)	HABANA	AIJM	T3	LOCAL INT.	1	1.7	8
	LOST AND FOUND - T3	HABANA	AIJM	T3	LOCAL INT.	1	1.7	9
	JEFE LÍNEA AÉREA - T3 y, OFICINAS LÍNEA AÉREA	HABANA	AIJM	T3	LOCAL INT.	2	1.7	9
	ATENCIÓN A PASAJEROS y VENTA BOLETOS (LOCAL VENTAS)	HABANA	AIJM	T3	LOCAL INT.	2	1.7	9
	PROTECCIÓN A VUELOS CUBANA (GESTIÓN DE ESCOLTAS)	HABANA	AIJM	T3	CONTENEDOR	1	1.7	9
	PROTECCIÓN A VUELOS CUBANA (ANÁLISIS EQUIPAJES)	HABANA	AIJM	T3	LOCAL INT.	1	1.7	10
	DEPARTAMENTO DE CUBANA CARGO	HABANA	AIJM	AERO VARADERO	DPTO. CARGA	1-2	1.8	11
	- PLANTA BAJA	HABANA	AIJM	AERO	DPTO. CARGA	1	1.8	11

				VARADERO				
	- PLANTA ALTA	HABANA	AIJM	AERO VARADERO	DPTO. CARGA	2	1.8	11
	DEPARTAMENTO DE CUBANA CARGO	HABANA	AIJM	AERO VARADERO	CENTRO NEGOCIOS	2	1.9	12
	CONTENEDOR CUBANA CARGO	HABANA	AIJM	AERO VARADERO	CENTRO NEGOCIOS	1	1.9	12
	EDIFICIO PRINCIPAL TAR HABANA	HABANA	AIJM	TARHAV	EDIF. TAR	1-2	-	
	- PLANTA BAJA	HABANA	AIJM	TARHAV	EDIF. TAR	1	-	
	o DPTOS. INDEPENDIENTES (AUDITORIA y otros)	HABANA	AIJM	TARHAV	EDIF. TAR	1	1.10	13
	o DPTOS. ANTIGUOS TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	1	1.11	13
	o TEATRO TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	1	-	-
	o TALLERES MECANICA EMPRESA	HABANA	AIJM	TARHAV	EDIF. TAR	1	-	-
	- PLANTA ALTA	HABANA	AIJM	TARHAV	EDIF. TAR	2	-	-
	o NODO TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.11	14
	o DPTO. INFORMATICA TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.11	14
	o DIRECCIÓN GENERAL EMPRESA	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o PRIMERA DIRECCION GENERAL ADJUNTA	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o PUESTO DE MANDO	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o OCIC	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o SALONES DE REUNIONES	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o DPTOS. INDEPENDIENTES (SUPERVISION y otros)	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.10	13
	o DIRECCION VICEPRESIDENCIA TECNICA	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.12	13
	o DPTOS. SUBDIRECCION INGENIERIA	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.12	13
	o DIRECCION TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.11	13
	o DPTOS. ANTIGUOS TAR HAV	HABANA	AIJM	TARHAV	EDIF. TAR	2	1.11	13
	DPTOS. TALLERES TÉCNICOS	HABANA	AIJM	TARHAV	EDIF. TAR	1	1.11	13
	- EDIFICIO A (IZQUIERDA, MIRANDO HACIA PISTA APTO)	HABANA	AIJM	TARHAV	EDIF. TAR	1	1.11	13
	- EDIFICIO B (DERECHA, MIRANDO HACIA PISTA APTO)	HABANA	AIJM	TARHAV	EDIF. TAR	1	1.11	13
	HANGAR	HABANA	AIJM	TARHAV	HANGAR	1	1.11	13
	DIRECCIÓN MANTENIMIENTO DE LÍNEA (MTTO. LINEA, FIABILIDAD y DIAGNÓSTICO MOTORES)	HABANA	AIJM	MTTO. LINEA	MTTO. LINEA	1	1.23	27
	ALMACENES ATM	HABANA	AIJM	UIMA	UIMA	1	1.14	15
	ATENCIÓN VUELOS ALBA	HABANA	AIJM	T5	T5	1	1.15	16
	OFICINA COMERCIAL DE VENTA PARA VUELOS INTERNACIONALES	HABANA	LA RAMPA	RAM	CACSA	1	1.16	-
	o NACSI (NODO ALTERNATIVO CENTRAL PARA CONTINGENCIA DE SERVICIOS INFORMÁTICOS)	HABANA	LA RAMPA	RAM	CACSA	1	1.0	17
	o AREA DE VENTAS DE BOLETOS	HABANA	LA RAMPA	RAM	CACSA	1	1.16	18
	o DPTO. VENTAS POR INTERNET (COMERCIO ELECTRONICO)	HABANA	LA RAMPA	RAM	CACSA	1	1.16	18

	OFICINA COMERCIAL DE VENTAS PARA VUELOS NACIONALES	HABANA	LA RAMPA	RAM	HUMBOLDT	1-2	1.16	-
	- PLANTA ALTA	HABANA	LA RAMPA	RAM	HUMBOLDT	2	1.16	19
	- PLANTA BAJA	HABANA	LA RAMPA	RAM	HUMBOLDT	1	1.16	19
	OFICINA COMERCIAL DE VENTAS DE 5ta. Y 110.	HABANA	MIRAMAR	5TA&110	TAKE-OFF	1	1.17	20
	OFICINA COMERCIAL DE VENTAS EN VARADERO (VRA)	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	1-2	1.18	21
	- PLANTA BAJA	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	1	1.18	21
	○ CENTRO DE DATOS ○ (NODO DE SERVICIOS DE TICs)	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	1	1.18	21
	○ AREA DE VENTAS DE BOLETOS	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	1	1.18	21
	- PLANTA ALTA	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	2	1.18	21
	○ DIRECCIÓN, CONTABILIDAD y otros.	VARADERO	CIUDAD	OFICINA VRA	OFICINA VRA	2	1.18	21
	OFICINA DE APTO (S-TIC por EMPRESA ECASA)	VARADERO	APTO	APTO	LOCAL AEROP.	2	-	-
	OFICINA COMERCIAL DE VENTAS EN CIENFUEGOS (CFG)	CIENFUEGOS	CIUDAD	CENTRO NEG.AUSA	INMOBILIARIA AUSA	1	1.18	22
	OFICINA COMERCIAL DE VENTAS EN CAMAGÜEY (CMW)	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	1-2	1.19	23
	- PLANTA BAJA	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	1	1.19	23
	○ CENTRO DE DATOS ○ (NODO DE SERVICIOS DE TICs)	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	1	1.19	23
	○ AREA DE VENTAS DE BOLETOS y OTROS	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	1	1.19	23
	- PLANTA ALTA	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	2	1.19	23
	○ DIRECCIÓN, CONTABILIDAD y otros.	CAMAGÜEY	CIUDAD	OFICINA CMW	OFICINA CMW	2	1.19	23
	OFICINA DE APTO (S-TIC por EMPRESA ECASA)	CAMAGÜEY	APTO	APTO	LOCAL AEROP.	2	-	-
	OFICINA COMERCIAL DE VENTAS EN HOLGUIN (HOG)	HOLGUIN	CIUDAD	OFICINA HOG	OFICINA HOG	1-2	1.20	24
	- PLANTA BAJA	HOLGUIN	CIUDAD	OFICINA HOG	OFICINA HOG	1	1.20	24
	○ CENTRO DE DATOS ○ (NODO DE SERVICIOS DE TICs)	HOLGUIN	CIUDAD	OFICINA HOG	OFICINA HOG	1	1.20	24
	○ AREA DE VENTAS DE BOLETOS y OTROS	HOLGUIN	CIUDAD	OFICINA HOG	OFICINA HOG	1	1.20	24
	OFICINA DE APTO (S-TIC por EMPRESA ECASA)	CAMAGÜEY	APTO	APTO	LOCAL AEROP.	2	-	-
	OFICINA COMERCIAL DE VENTAS EN STGO. DE CUBA (SCU)	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	1-2	1.21	25
	- PLANTA BAJA	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	1	1.21	25
	○ CENTRO DE DATOS ○ (NODO DE SERVICIOS DE TICs)	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	1	1.21	25
	○ AREA DE VENTAS DE BOLETOS y OTROS	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	1	1.21	25
	- PLANTA ALTA	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	2	1.21	25
	○ DIRECCIÓN, CONTABILIDAD y OTROS.	STGO. CUBA	CIUDAD	OFICINA SCU	OFICINA SCU	2	1.21	25

	OFICINA DE APTO (S-TIC por EMPRESA ECASA)	STGO. CUBA	APTO	APTO	LOCAL AEROP.	2	-	-
	TALLER AERONÁUTICO REPARACIONES TAR SCU (DESACTIVADO EN AÑO 2012)	STGO. CUBA	APTO	APTO	EDIF. AEROP.	-	-	-

TOTAL DE PSIs EN TERRITORIO NACIONAL: 23

TOTAL DE ANALISIS DE RIESGOS ESPECIFICOS IDENTIFICADOS ACORDE A AREAS EN TERRITORIO NACIONAL: 27

Fuera del territorio de la República de Cuba

ID	LOCALIZACIÓN	REGION	ZONA	AREA	EDIF.	NIVEL	PSI	ANAL. RIESGOS
	EUROPA							
01	OFICINA COMERCIAL DE VENTAS EN MADRID (MAD)	ESPAÑA	MADRID	-			1	
	- OFICINA DE CIUDAD	ESPAÑA	MADRID	CIUDAD			1	1
	- OFICINA EN APTO PARA DICHA CIUDAD	ESPAÑA	MADRID	APTO			1	1
02	OFICINA COMERCIAL DE VENTAS EN PARIS (PAR)	FRANCIA	PARIS	-			2	
	- OFICINA DE CIUDAD	FRANCIA	PARIS	CIUDAD			2	2
	- OFICINA EN APTO PARA DICHA CIUDAD	FRANCIA	PARIS	APTO			2	2
03	OFICINA COMERCIAL DE VENTAS EN ROMA (ROM)	ITALIA	ROMA	-			3	
	- OFICINA DE CIUDAD	ITALIA	ROMA	CIUDAD			3	3
	AMERICA DEL NORTE							
04	OFICINA COMERCIAL DE VENTAS EN TORONTO (YYZ)	CANADA	TORONTO	-			4	
	- OFICINA DE CIUDAD	CANADA	TORONTO	CIUDAD			4	4
	- OFICINA EN APTO PARA DICHA CIUDAD	CANADA	TORONTO	APTO			4	4
05	OFICINA COMERCIAL DE VENTAS EN MONTREAL (YUL)	CANADA	MONTREAL	-			5	
	- OFICINA DE CIUDAD	CANADA	MONTREAL	CIUDAD			5	5
	- OFICINA EN APTO PARA DICHA CIUDAD	CANADA	MONTREAL	APTO			5	5
06	OFICINA COMERCIAL DE VENTAS EN MÉXICO DF (MEX)	MÉXICO	D.F.	-			6	
	- OFICINA DE CIUDAD	MÉXICO	D.F.	CIUDAD			6	6
	- OFICINA EN APTO PARA DICHA CIUDAD	MÉXICO	D.F.	APTO			6	6
07	OFICINA COMERCIAL DE VENTAS EN CANCÚN (CUN)	MÉXICO	CANCÚN	-			7	
	- OFICINA DE CIUDAD	MÉXICO	CANCÚN	CIUDAD			7	7
	- OFICINA EN APTO PARA DICHA CIUDAD	MÉXICO	CANCÚN	APTO			7	7
	CENTRO AMERICA Y CARIBE							
08	OFICINA COMERCIAL DE VENTAS EN BAHAMAS (NAS)	BAHAMAS	NASSAU	-			8	
	- OFICINA DE CIUDAD	BAHAMAS	NASSAU	CIUDAD			8	8
09	OFICINA COMERCIAL DE VENTAS EN COSTA RICA (SJO)	COSTA RICA	SAN JOSÉ	-			9	

	- OFICINA DE CIUDAD	COSTA RICA	SAN JOSÉ	CIUDAD			9	9
10	OFICINA COMERCIAL DE VENTAS EN REP. DOM. (SDQ)	REP. DOM.	STO. DOMINGO	-			10	
	- OFICINA DE CIUDAD	REP. DOM.	STO. DOMINGO	CIUDAD			10	10
	- OFICINA EN APTO PARA DICHA CIUDAD	REP. DOM.	STO. DOMINGO	APTO			10	10
11	OFICINA COMERCIAL DE VENTAS EN PANAMÁ (PTY)	PANAMÁ	CDAD. PANAMÁ	-			11	
	- OFICINA DE CIUDAD	PANAMÁ	CDAD. PANAMÁ	CIUDAD			11	11
12	OFICINA COMERCIAL DE VENTAS EN NICARAGUA (MGA)	NICARAGUA	MANAGUA	-			12	
	- OFICINA DE CIUDAD	NICARAGUA	MANAGUA	CIUDAD			12	12
	- OFICINA EN APTO PARA DICHA CIUDAD	NICARAGUA	MANAGUA	APTO			12	12
13	OFICINA COMERCIAL DE VENTAS EN HONDURAS (SPA)	HONDURAS	SAN PEDRO ZULA	-			13	
	- OFICINA DE CIUDAD	HONDURAS	SAN PEDRO ZULA	CIUDAD			13	13
	- OFICINA EN APTO PARA DICHA CIUDAD	HONDURAS	SAN PEDRO ZULA	APTO			13	13
14	OFICINA COMERCIAL DE VENTAS EN HAITÍ (PAP)	HAITÍ	PUERTO PRÍNCIPE				14	
	- OFICINA DE CIUDAD	HAITÍ	PUERTO PRÍNCIPE	CIUDAD			14	14
	- OFICINA EN APTO PARA DICHA CIUDAD	HAITÍ	PUERTO PRÍNCIPE	APTO			14	14
	AMERICA DEL SUR							
15	OFICINA COMERCIAL DE VENTAS EN VENEZUELA (CCS)	VENEZUELA	CARACAS	-			15	
	- OFICINA DE CIUDAD	VENEZUELA	CARACAS	CIUDAD			15	15
	- OFICINA EN APTO PARA DICHA CIUDAD	VENEZUELA	CARACAS	APTO			16	15
16	OFICINA COMERCIAL DE VENTAS EN ARGENTINA (BUE)	ARGENTINA	CANCUN	-			16	
	- OFICINA DE CIUDAD (BUE)	ARGENTINA	BUENOS AIRES	CIUDAD			16	16
	- OFICINA EN APTO PARA DICHA CIUDAD (EZE)	ARGENTINA	BUENOS AIRES	APTO			16	16
17	OFICINA COMERCIAL DE VENTAS EN BRASIL (SAO)	BRASIL	SAO PAULO	-			17	
	- OFICINA DE CIUDAD	BRASIL	SAO PAULO	CIUDAD			17	17
18	OFICINA COMERCIAL DE VENTAS EN COLOMBIA (BOG)	COLOMBIA	BOGOTA	-			18	
	- OFICINA DE CIUDAD	COLOMBIA	BOGOTA	CIUDAD			18	18
19	OFICINA COMERCIAL DE VENTAS EN ECUADOR (UIO)	ECUADOR	QUITO	-			19	
	- OFICINA DE CIUDAD	ECUADOR	QUITO	CIUDAD			19	19
20	OFICINA COMERCIAL DE VENTAS EN MARTINICA (PTP)	MARTINICA	PORT de PEAR	-			20	
	- OFICINA EN APTO PARA DICHA CIUDAD	MARTINICA	PORT de PEAR	APTO			20	20

TOTAL DE PSIs EN TERRITORIO NACIONAL: 20

TOTAL DE ANALISIS DE RIESGOS ESPECIFICOS IDENTIFICADOS ACORDE A AREAS EN TERRITORIO NACIONAL: 20

Anexo 7 Políticas establecidas para el Sistema de Gestión de Seguridad de la Información (SGSI).

Políticas del Sistema de Gestión de Seguridad de la Información (SGSI) para las Tecnologías de la Información (Informática y Comunicaciones) para las dependencias de Cubana de Aviación S.A. (v4.2.5 – Abr2014)		
Notación para los contenidos: C : categoría S : subcategoría P : Política		
Referencia	Tipo	Descripción
1	C	General
1.1	P	Ambito de cumplimiento de la Resolución 127/2007
1.2	P	Prioridad y niveles de las regulaciones
1.3	P	Roles en la organización con competencia en las TICs
1.4	P	Roles en la organización con competencia y responsabilidad en el SGSI y en los PSI
2	C	Política de seguridad de la información en las TICs
2.1	P	Requisito de existencia del PSI como documento del SGSI
2.2	P	Revisión y mejora del SGSI en las UE
3	C	Organización de la seguridad de la información en las TICs
3.A	S	<i>Organización interna</i>
3.A.1	P	Compromiso con el SGSI y tipos de evidencia para la evaluación de dicho compromiso
3.A.2	P	Acceso a los recursos de información y servicios
3.B	S	<i>Partes externas</i>
3.B.1	P	Riesgos de empleo de partes externas o terceros
3.B.2	P	Acuerdos con terceras partes y relación con el SGSI de la organización
4	C	Gestión de activos

4.A	S	<i>Responsabilidad por los activos</i>
4.A.1	P	Identificación y control de los activos
4.A.2	P	Exigencia de responsable por cada bien informático
4.A.3	P	Fin de utilización de los bienes informáticos
4.A.4	P	Regulaciones asociadas al uso de bienes informáticos
4.B	S	<i>Clasificación de la Información</i>
4.B.1	P	Competencia en la clasificación de la información
5	C	Seguridad de Recursos Humanos
5.A	S	<i>Antes del Empleo</i>
5.A.1	P	Selección de personal que atiende las TICs
5.A.2	P	Terceros y el SGSI de la organización
5.B	S	<i>Durante el Empleo</i>
5.B.1	P	Aceptación del compromiso por parte del personal con el SGSI
5.B.2	P	Educación, formación y toma de conciencia del personal respecto del SGSI
5.C	S	<i>Terminación o cambio de Empleo</i>
5.C.1	P	Responsabilidades de los roles de la entidad
6	C	Seguridad Física y Ambiental
6.A	S	<i>Areas Seguras</i>
6.A.1	P	Características para las áreas que contengan recursos de información
6.A.2	P	Medios protección contra desastres
6.B	S	<i>Seguridad de los Equipos</i>
6.B.1	P	Sellos de seguridad para los equipos

6.B.2	P	Protección eléctrica
6.B.3	P	Protección de cables
6.B.4	P	Mantenimiento de los equipos
6.B.5	P	Equipamiento fuera de las instalaciones
6.B.6	P	Destrucción segura de información en equipamiento
6.B.7	P	Uso fuera de la instalación de la entidad
7	C	Gestión de Comunicaciones y Operaciones
7.A	S	<i>Procedimientos y Responsabilidades de Operación</i>
7.A.1	P	Autorización de acceso a recursos de información
7.B	S	<i>Gestión de entrega de servicio de una tercera parte</i>
7.B.1	P	Acuerdos legales con la tercera parte
7.B.2	P	Comprobación del cumplimiento de los acuerdos
7.C	S	<i>Protección contra código malicioso y movable</i>
7.C.1	P	Software de aplicaciones para la protección
7.C.2	P	Políticas para las soluciones antivirus
7.C.3	P	Solución antivirus propuesta
7.C.4	P	Gestión del código maligno
7.C.5	P	Estandarización del software utilizado
7.C.6	P	Tratamiento para el código movable
7.D	S	<i>Copia de seguridad</i>
7.D.1	P	Existencia
7.D.2	P	Recursos
7.D.3	P	Designación de responsabilidad
7.D.4	P	Verificación de integridad

7.D.5	P	Registro de operación
7.D.6	P	Recomendaciones para la gestión de copia
7.D.7	P	Periodicidad
7.D.8	P	Número de copias y gestión de las mismas
7.D.9	P	Eliminación
7.E	S	<i>Gestión de seguridad en la red</i>
7.E.1	P	Area de equipos críticos
7.E.2	P	Personal y autorización para área de equipos críticos
7.E.3	P	Seguridad física para área crítica
7.E.4	P	Area crítica y áreas públicas
7.E.5	P	Equipamiento en área crítica
7.E.6	P	Clima en área crítica
7.E.7	P	Sistemas de protección en área crítica
7.E.8	P	Sistemas protección contra desastres en área crítica
7.E.9	P	Sistemas de vigilancia
7.E.10	P	Uso de medios de almacenamiento en área crítica
7.F	S	<i>Manejo de medios de información</i>
7.F.1	P	Medios de almacenamiento movibles
7.F.2	P	Destrucción de la información en medios
7.F.3	P	Almacenamiento administrado de información del negocio
7.F.4	P	Almacenamiento de la información del negocio en estaciones de usuarios
7.F.5	P	Procedimiento de manejo de la información
7.F.6	P	Documentación de sistemas y su seguridad
7.G	S	<i>Intercambio de información</i>
7.G.1	P	Medios de Información en Tránsito

7.G.2	P	Servicio de Correo
7.G.3	P	Mensaje Electrónico
7.G.4	P	Sistemas de información del negocio
7.H	S	<i>Servicios de comercio electrónico</i>
7.H.1	P	Información disponible públicamente
7.I	S	<i>Seguimiento</i>
7.I.1	P	Registro de auditoría y período de preservación de los registros
7.I.2	P	Seguimiento de la utilización de los sistemas
7.I.3	P	Protección de la información de registro
7.I.4	P	Seguimiento de registros asociados a actividad de administrador y operador de registros
7.I.5	P	Registro de fallas
7.I.6	P	Sincronización de relojes
8	C	Control de Accesos
8.A	S	<i>Requisitos del negocio para el control de los accesos</i>
8.A.1	P	Política de control de accesos
8.B	S	<i>Gestión de acceso de usuarios</i>
8.B.1	P	Registro de usuarios
8.B.2	P	Revisión de los derechos de acceso de usuario
8.C	S	<i>Responsabilidades de los usuarios</i>
8.C.1	P	Uso de contraseñas
8.C.2	P	Equipo desatendido
8.D	S	<i>Control de acceso a la red</i>
8.D.1	P	Política de utilización de los servicios de red
8.D.2	P	Autenticación de usuarios y uso de recursos de información para

		conexiones externas
8.D.3	P	Protección del diagnóstico remoto y de la configuración de puerto
8.D.4	P	Segregación en redes
8.E	S	<i>Control de acceso al sistema operativo</i>
8.E.1	P	Requisito de procedimientos de conexión segura
8.E.2	P	Identificación y autenticación del usuario
8.E.3	P	Sistema de gestión de contraseñas
8.E.4	P	Uso de las prestaciones del sistema para fines inadecuados
8.E.5	P	Limitación del tiempo de conexión
8.F	S	<i>Computación móvil y trabajo a distancia</i>
8.F.1	P	Computación móvil y comunicaciones
8.F.2	P	Trabajo a distancia
9	C	Adquisición, desarrollo y mantenimiento de sistemas de información
9.A	S	<i>Requisitos de seguridad de los sistemas de información</i>
9.A.1	P	Análisis y especificación de los requisitos de seguridad
9.B	S	<i>Controles criptográficos</i>
9.B.1	P	Política sobre la utilización de controles criptográficos
9.C	S	<i>Seguridad de los archivos del sistema</i>
9.C.1	P	Control del software operativo
9.D	S	<i>Seguridad en los procesos de desarrollo y soporte</i>
9.D.1	P	Revisión técnica de las aplicaciones si hay cambios previstos en el sistema operativo
9.D.2	P	Restricciones en los cambios a paquetes de software
10	C	Gestión de incidente de seguridad de la información

10.A	S	<i>Reportar los incidentes y debilidades de seguridad de la información</i>
10.A.1	P	Reporte de los incidentes y eventos de seguridad de la información
10.A.2	P	Reporte de debilidades de la seguridad
10.B	S	<i>Gestión de los incidentes y mejoras de seguridad de la información</i>
10.B.1	P	Recolección de evidencias
11	C	Gestión de continuidad del negocio
11.A	S	<i>Aspectos de seguridad de la información de la gestión de continuidad del negocio</i>
11.A.1	P	Continuidad del negocio y evaluación del riesgo
11.A.2	P	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información
11.A.3	P	Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio
12	C	Cumplimiento
12.A	S	<i>Cumplimiento de requisitos legales</i>
12.A.1	P	Identificación de la legislación aplicable
12.A.2	P	Derechos de propiedad intelectual, recomendación de empleo de open source
12.A.3	P	Prevención del mal uso de los recursos de procesamiento de la información
12.B	S	<i>Cumplimiento con las políticas y normas de seguridad y el cumplimiento técnico</i>
12.B.1	P	Cumplimiento con las políticas y normas de seguridad
12.B.2	P	Comprobación del cumplimiento técnico
12.C	S	<i>Consideraciones de auditoría de los sistemas de información</i>
12.C.1	P	Controles de auditoría de los sistemas de información

12.C.2	P	Protección de las herramientas de auditoría de los sistemas de información y los registros de las mismas
13	C	De la inspección a la seguridad de las Tecnologías de Información y Comunicaciones
13.A	S	<i>Personal de las inspecciones</i>
13.A.1	P	Personal con competencia y designación para la inspección
13.A.2	P	Preparación complementaria del personal para la verificación del SGSI

Referencias bibliográficas:

- ISO/IEC 17799 Estándar internacional sobre Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.
- ISO/IEC 27001 Estándar internacional sobre Tecnología de la Información – Técnicas de seguridad – Sistema de Gestión de Seguridad de la Información – Requisitos.
- Resolución 127/2007 (en lo adelante Res. 127) Reglamento de Seguridad de las Tecnologías de Informática y Comunicaciones, conocida también como Seguridad Informática del Ministerio de Informática y Comunicaciones (MIC) de la República de Cuba. Basado en estándares internacionales como los mencionados con anterioridad.
- Resolución 60/11 – Contraloría General de la República de Cuba, La Habana, 3 de marzo del 2011, Año CIX, Núm. 13, Pág. 39 (<http://www.gacetaoficial.cu>)

Términos:

- **Política:** Intención y dirección general expresada formalmente por la gerencia (ISO/IEC 17799)
- **Control:** 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. (ISO/IEC 17799)

- **Lineamiento:** Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas. (ISO/IEC 17799)
- **Activo:** Cualquier cosa que tenga valor para la organización. (ISO/IEC 17799)
- **Tercera Persona:** Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión. (ISO/IEC 17799)
- **Dueño:** Este término identifica a un individuo o entidad que tiene responsabilidad de gestión aprobada para controlar la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término “dueño”no significa que la persona actualmente tiene derechos de propiedad sobre el activo. (ISO/IEC 27001).

Nota: En determinados contextos socioeconómicos este término es sinónimo de “**responsable**”.

- **Empleo:** La palabra “Empleo” significa cubrir todas las diferentes situaciones siguientes: empleo de personas (temporal o contratada), la asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos arreglos. (ISO/IEC 27001).

Nota: En nuestro contexto “roles de trabajo” tiene como sinónimo “funciones del cargo”.

- **Negocio:** De manera general, las referencias a “Negocio” en este documento, deben ser interpretadas como: “Aquellas actividades que son medulares o esenciales a los propósitos de la existencia de la organización”. (ISO/IEC 27001)
- **PSI:** Documento del Plan de Seguridad Informática.
- **CACSA:** Corporación de la Aviación Civil de Cuba, S.A.
- **DTCI-CACSA:** Departamento de Tecnologías de la Información y Comunicaciones de CACSA.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **TIC:** Tecnologías de la Información y las Comunicaciones