ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA DE UN MODELO DE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA INSTITUTOS SUPERIORES TECNOLOGICOS DE EDUCACION AERONAUTICA

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER (MSc) EN
GESTION DE LAS COMUNICACIONES
Y
TECNOLOGÍAS DE LA INFORMACIÓN

PATRICIO EDUARDO CHACON MEJIA
chacon_patricio@hotmail.com

DIRECTOR: MSc. Ing. Gustavo Samaniego
gustavo.samaniego@epn.edu.ec

Quito, Septiembre 2008

DECLARACIÓN

Yo PATRICIO EDUARDO CHACON MEJIA, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

PATRICIO EDUARDO CHACON MEJIA

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Patricio Eduardo Chacón Mejía, bajo mi supervisión.

Ing. MSc. Gustavo Samaniego

DIRECTOR DE PROYECTO

RESUMEN

El objetivo de este trabajo de tesis es elaborar una propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información para Institutos de Educación Superior Tecnológica Aeronáutica en el Ecuador. Primero, fue necesario conocer el estado actual de los Riesgos y de la Gestión de Seguridad de la Información en estos Institutos, en base a encuestas y entrevistas, cuyos resultados fueron analizados y procesados en forma cualitativa; se agruparon los datos según su naturaleza y se los evaluó posteriormente.

El levantamiento de los riesgos fue en base a considerar los principios fundamentales que comprometen a la seguridad de la información, que son: disponibilidad, confidencialidad y la integridad.

El resultado de las encuestas permitió identificar los riesgos, considerando su orden de importancia , así como las debilidades detectadas en la gestión de la seguridad de la información; por lo que con este análisis y fundamentados en el propósito de demostrar que es factible realizar una gestión competente, efectiva y continua de la seguridad en el marco de los riesgos detectados y de que se pueden adoptar las medidas adecuadas en proporción a la magnitud y tipo de organización, se identificaron los requerimientos de Seguridad de la Información.

Posteriormente se analiza y estudia la serie de la norma ISO 27000, determinando usar combinadamente el Estándar ISO:27002 (mejores practicas) que no es certificable, con el Estándar ISO:27001 certificable, para realizar la construcción del Modelo de Sistema de Gestión de Seguridad de la Información SGSI en estos Centros de Enseñanza Aeronáutica, ya que se adaptan a la naturaleza cambiante en estructura y procesos de ellos.Y también porque la necesidad de profesionalizar los centros de instrucción en materia de aeronáutica civil del Ecuador ha incrementado la utilización de tecnologías de información sin contar con una normatividad o reglamentación orientada a proteger sus activos.

Entonces al partir de la hipótesis de trabajo: “Es posible gestionar adecuadamente la seguridad de la información en los institutos de educación superior aeronáutica, mediante un Sistema de Gestión de Seguridad de la Información” en el desarrollo de este proyecto se efectúan los análisis para demostrar lo indicado; señalando los pasos necesarios que son:

- Aplicar la metodología de análisis de riesgo propuesta, con el fin de valorar los bienes informáticos, prever amenazas, conocer vulnerabilidades y efectuar un análisis costo beneficio.
- Utilizar y adaptar las políticas de seguridad recomendadas, los controles y los objetivos de control propuestos por la norma ISO 27001:2005 a los establecimientos de instrucción aeronáutica en general y su entorno para gestionar sus procesos.

Justificándose de esta manera la fundamentación doctrinaria utilizada en el desarrollo de esta tesis, que confluye a determinar los requerimientos de implantación y su posterior evaluación de la aplicabilidad de la propuesta.

Finalmente se formulan algunas conclusiones y se propone las recomendaciones.

DEDICATORIA

A quien me sigue brindando sus bendiciones .

Patricio.

INTRODUCCION

La capacitación es un elemento esencial en la aeronáutica, bien planificada y estratégicamente diseñada contribuirá a asegurar el orden y la seguridad para el crecimiento de la aviación en el siglo XXI.

La complejidad de los nuevos sistemas y el advenimiento de procedimientos operativos sofisticados traen como consecuencia la necesidad de profesionalizar los centros de instrucción aeronáutica. En el Ecuador la formación aeronáutica, básicamente tiene la peculiaridad de ser una instrucción de corta duración, en función de la necesidad de integrar rápidamente el Recurso Humano en áreas propias de esta actividad para los sectores de aviación civil, militar, compañías de aviación etc., etc., especialmente en las áreas de Transito Aéreo, Operaciones de Vuelo, Meteorología e Informática, Seguridad de Aviación, Mecánica Aeronáutica.

En la mayoría de estos institutos, los departamentos de informática o afines, no disponen de un Modelo que oriente a las personas responsables del área de Sistemas sobre las mejores prácticas para salvaguardar la información confiada a los Sistemas de Información, hay una falta de conocimiento de los mecanismos tecnológicos que resguarden la información, y de las tendencias tecnológicas para protegerse, contra amenazas y ataques tanto internas como externas a la organización.

La utilización de un modelo para hacer la gestión de la Seguridad de la Información, facilitará un cambio socio-cultural con responsabilidad y eficacia en los Centros de Instrucción Aeronáutica.

El aumento de las amenazas en contra de la información que circula en las redes locales se multiplican, y aún en nuestro medio todavía no se ha creado una conciencia del riesgo que implica mantener redes desprotegidas, peor aún de

disponer de las políticas de seguridad informática que norman los institutos internacionales de normalización, para que así se eviten cuantiosas pérdidas económicas.

El objetivo general en el desarrollo de la presente tesis es: **Elaborar una propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información para Institutos de Educación Superior Tecnológica Aeronáutica.** Esto se pretende lograr mediante la consecución de los siguientes objetivos específicos:

- Analizar la actual situación del manejo de la información en los institutos tecnológicos superiores de educación aeronáutica

- Construir el Modelo de Sistema de Gestión de Seguridad de la Información SGSI.

- Validar la aplicabilidad de la propuesta en el ISTAC Instituto Superior Tecnológico de Aviación Civil.

El sistema de gestión de la seguridad de la información (SGSI) es la parte del sistema de gestión de la empresa u organización en general, basado en un enfoque de riesgos del negocio, para:

- establecer,
- implementar,
- operar,
- monitorear,
- mantener y mejorar la seguridad de la información.

Paulatinamente la investigación se enfoca a conocer el estado de la gestión de la seguridad de la información en estos centros de educación aeronáutica e identificar los riesgos a los que están expuestos. Con este propósito, se utiliza dos encuestas en base a la adaptación del Modelo Consultative, Objetive and

Bifuncional Risk de la empresa norteamericana C&A Systems Security Ltd las mismas que fueron elaboradas en base a la norma ISO 17799.

El objetivo de un Modelo es poner orden y estructura de los procesos en general, en este caso el de seguridad, para el propósito de nuestro Modelo se plantea la utilización y adaptación de la Norma ISO 27001:2005 al entorno de los Institutos de Educación Aeronáutica en el Ecuador. En este proyecto sugerimos se utilice las partes que mediante un análisis pragmático de la norma y otras mejores practicas, permitieron el gestionar adecuadamente las políticas y procedimientos de seguridad que se sugiere utilicen estos centros de enseñanza aeronáutica.

CONTENIDO

CAPITULO I 12

1 SITUACION ACTUAL DEL MANEJO DE INFORMACION. 12

1.1 RIESGOS EN EL MANEJO DE INFORMACIÓN EN LOS INSTITUTOS TECNOLÓGICOS SUPERIORES DE EDUCACIÓN AERONÁUTICA..... 13
1.1.1 EL ANÁLISIS DE RIESGO 13
1.1.2 METODOLOGÍA DE ANÁLISIS DE RIESGOS 15

1.2 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION 23
1.2.1 RIESGOS IDENTIFICADOS QUE PODRIAN AFECTAR A LOS INSTITUTOS TECNOLOGICOS DE EDUCACION AERONAUTICA 27
1.2.2 IDENTIFICACION Y CLASIFICACIÓN DE LA INFORMACION EN SUS FORMAS Y MEDIOS DE ACUERDO A SU CRITICIDAD 31
1.2.3 VINCULO DE LA CLASIFICACIÓN DE LA INFORMACIÓN CON LAS POLÍTICAS Y PROCEDIMIENTOS. 34

CAPITULO II 35

2 ELABORACION DE LA PROPUESTA DEL MODELO DE SGSI 35

2.1 ELABORACION DE LA PROPUESTA DEL MODELO DE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION 36
2.1.1 TERMINOS Y DEFINICIONES 36
2.1.2 APLICACIÓN DE LA NORMA ISO 27001: 2005 36
2.1.3 LA SERIE 27000 39
2.1.4 PROPUESTA DEL MODELO SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI 43

2.2 REQUERIMIENTOS DE IMPLANTACION DEL SISTEMA DE SEGURIDAD DE INFORMACION 67
2.2.1 INVOLUCRAMIENTO DE LA ALTA DIRECCION 68
2.2.2 EQUIPO DE IMPLANTADORES (STAKEHOLDERS) 69
2.2.3 SOFTWARE 70
2.2.4 MANTENIMIENTO Y ADMINISTRACION 71
2.2.5 DISPONIBILIDAD 24X7 71
2.2.6 REGLAMENTACIONES O DISPOSICION LEGALES 72
2.2.7 SOCIALIZACIÓN DEL MODELO 72

CAPITULO III 74

3 EVALUACION DE LA APLICABILIDAD DE LA PROPUESTA 74

3.1 EN EL ASPECTO LEGAL 75

3.2 EN EL ASPECTO ORGANIZACIONAL 77

3.3 EN EL ASPECTO OPERACIONAL 80

3.4 EN EL ASPECTO ECONOMICO 81

CAPITULO 4 85

4 CONCLUSIONES Y RECOMENDACIONES 85

4.1 CONCLUSIONES 85

4.2 RECOMENDACIONES 87

BIBLIOGRAFIA 89

ANEXOS 91

CAPITULO I

1 SITUACION ACTUAL DEL MANEJO DE INFORMACION.

INTRODUCCION

La información es clave para el crecimiento y el éxito de una Institución Educativa. Un Sistema de Gestión de Seguridad de la Información demuestra a los usuarios que su información cuenta con protección adecuada: ya sea que esté almacenada o en papel, en formato electrónico o en las mentes de sus usuarios.

Un Sistema de Gestión de Seguridad de la Información ayuda a identificar y reducir riesgos vitales de seguridad, ya que permite centrar los esfuerzos en la seguridad de la información y protegerla.

Este capitulo presenta la metodología utilizada, para efectuar un análisis de los riesgos que pueden afectar a la seguridad de la información basados en las encuestas y también de manera heurística [1]

La norma ISO 27001:2005 sigue un enfoque detallado hacia la seguridad de la información. Activos que necesitan un ámbito de protección desde información digital, documentos en papel, y activos físicos (computadoras y redes) para el conocimiento de cada usuario. Cuestiones que hay que abordar desde el desarrollo de competencia del personal hasta la protección técnica contra el fraude informático.

---

[1] *Es el arte de obtener una solución cercana a la óptima a problemas reales, en un tiempo razonable*

El uso de esta norma ayuda a proteger la información en términos de:

- Asegurar la **confidencialidad**, que la información está accesible solo para aquellas personas autorizadas a tener acceso.
- Proteger la **integridad** de la precisión y totalidad de la información y los métodos de tratamiento.
- Garantizar la **disponibilidad**, que los usuarios autorizados tengan acceso a la información y los activos relacionados cuando lo necesitan.

Aquí se hace una clasificación de los activos de información con respecto a sus niveles de sensibilidad. El propósito de la clasificación es indicar el nivel de confidencialidad, integridad y disponibilidad que es requerida para cada tipo de información. En este capítulo también se presentan los conceptos de clasificación de información, las limitaciones de aplicabilidad, y se indica una propuesta de clasificación de información.

1.1 RIESGOS EN EL MANEJO DE INFORMACIÓN EN LOS INSTITUTOS TECNOLÓGICOS SUPERIORES DE EDUCACIÓN AERONÁUTICA.

1.1.1 EL ANÁLISIS DE RIESGO

Es un paso importante para implementar la seguridad de la información. Como su propio nombre lo indica, es realizado para **detectar los riesgos** a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.

Las amenazas se pueden convertir en realidad a través de **fallas de seguridad**, que conocemos como **vulnerabilidades** y que deben ser eliminadas al máximo para que el ambiente que se desea proteger esté libre de riesgos de **incidentes** de seguridad.

Por lo tanto, la relación entre **amenaza-incidente-impacto**, es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para

la corrección de los **activos** que se desean proteger y deben ser siempre considerados cuando se realiza un análisis de riesgos.

Ejemplos de la relación amenaza-incidente-impacto:
Empecemos con el caso de la pérdida de un documento confidencial, que trae el listado de los principales deudores de una empresa. El incidente de la pérdida de esta información en sí es pequeño, pero el impacto que puede causar es inmenso, cuando se divulguen los nombres de las personas deudoras.
En el caso de la acción de una amenaza de un fenómeno meteorológico como el fenómeno del Niño, el incidente puede ser muy grande, pero si la institución cuenta con la protección adecuada en su infraestructura, el impacto puede ser pequeño.

Los resultados de un análisis de riesgo tienen como objetivo efectuar una comparación **costo beneficio**, para determinar si lo que se va ha invertir en seguridad de la información para proteger los activos, generará los beneficios necesarios para la continuidad del negocio o funcionamiento de la Institución, y la tranquilidad para los directivos y administradores de los Centros de Instrucción Aeronáutica.
Un análisis de riesgos demanda: identificar los bienes y sus amenazas, cuantificar el impacto en el negocio de las posibles amenazas, calcular el riesgo, establecer un balance entre el impacto que tendrá un riesgo y el costo de una contramedida.
Si una Institución no conoce que activos posee y su respectivo valor, tampoco puede saber cuanto tiene que invertir para proteger sus bienes. Los Directores, personal administrativo y usuarios de los Institutos deben conocer que el valor de un bien no solo es lo que costó adquirirlo, sino además: los costos de mantenimiento y protección, el valor que representa el bien para el Estado y el personal, el valor de la propiedad intelectual, el costo de reemplazo en caso de pérdida, las pérdidas de la producción si el bien no está disponible, la utilidad que genera, los costos de desarrollo de un producto, los costos de recuperación de un bien.

La Identificación de una amenaza implica conocer, cuales son los agentes que ocasionan una amenaza y la vulnerabilidad que puede ser explotada. Los agentes de amenaza que afectan la seguridad informática pueden ser: virus informáticos, hackers y sus derivaciones, usuarios, empleados, e intrusos.
Las vulnerabilidades que se pueden explotar pueden ser: la falta de una aplicación antivirus, pocas restricciones en la configuración del sistema operativo, mecanismos de control de acceso débiles, la carencia de una rigurosa configuración de un firewall, no existencia de auditorias informáticas, la falta de controles de ingresos electrónicos o guardias de seguridad.

1.1.2 METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología que se expone para el Análisis de Riesgos, se detalla en los siguientes pasos que se constituyen el punto central de la definición de un modelo de sistema de gestión de seguridad de la información, alineado con la misión y visión de la organización, dentro de su entorno de operación.

Esta metodología utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten tener valores aproximados para mayor precisión y exactitud, necesarios a la hora de tomar decisiones en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operatividad y continuidad del negocio de la organización.

1.1.2.1 Encuestas y Entrevistas

Mediante este tipo de aproximación a la organización, se busca entender los diferentes aspectos que la conforman, tanto en el aspecto tecnológico, como en los procesos que conforman su estructura organizacional, los cuales a su vez, son soportados por las aplicaciones y la infraestructura.
La normativa ISO 27001:2005 y su antecesora 17799, nos indica:

- Descripción de la Organización y sus Objetivos. Entendimiento de la organización, sus áreas funcionales y su ubicación geográfica.
- El levantamiento del detalle topológico de la infraestructura de tecnología existente, en el cual se especificará y detallará la plataforma de hardware, software, comunicaciones y procesos utilizados por los Institutos Superiores de Educación Aeronáutica.
- Listas de verificación de la Infraestructura Tecnológica: El objetivo de las listas de chequeo es identificar las vulnerabilidades de las plataformas tecnológicas.

1.1.2.2 Evaluación de riesgo

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la Información, sobre la plataforma tecnológica de los Institutos, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los elementos mencionados: **confidencialidad, disponibilidad e integridad**.

1.1.2.3 Determinación de la probabilidad

Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja, como se describe a continuación:

Nivel	Definición
Alta = 5	La amenaza es altamente motivada y es suficientemente capaz llevarse acabo
Media-Alta= 4	La amenaza está fundamentada y es posible
Media = 3	La amenaza es posible
Media-Baja = 2	La amenaza no posee la suficiente capacidad
Baja = 1	La amenaza no posee la suficiente motivación y capacidad

.

Tabla 1.1. Probabilidad de ocurrencia de un evento determinado.

Fuente: Escuela Politécnica del Ejército

1.1.2.4 Numero de ocurrencias del evento en el periodo de un año

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de electricidad, falla en las comunicaciones, utilizamos información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity News, www.cert.org, www.sans.org más la los resultados provenientes de experiencias observada en casos anteriores.

De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al numero de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5 se considera que ocurre al menos dos veces al año.

1.1.2.5 Identificación de vulnerabilidades

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se podría utilizar herramientas como listas de verificación y herramientas de software que determinan vulnerabilidades a nivel del sistema operativo y firewall:

Seguridad Física

- Monitoreo ambiental
- Controles de acceso
- Desastres naturales
- Control de incendios
- Inundaciones

Seguridad en las conexiones a Internet

- Políticas en el Firewall
- VPN
- Detección de intrusos
- Seguridad en la infraestructura de comunicaciones.
- Routers
- Switches
- Firewall
- Hubs
- RAS

Seguridad en Sistema Operativos (Unix, Windows, Linux)

Correo Electrónico

Seguridad en las aplicaciones Críticas

- Se define las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por: Sistemas operativos, hardware servidor, redes LAN y WAN, y el Departamento de Informática.

También con el fin de realizar una correspondencia con los datos obtenidos por medio de las listas de verificación, podemos mencionar que es factible, el uso de

una herramienta de software especializada, diseñada por la Empresa Norteamericana GFI Languard, la cual identifica vulnerabilidades en los sistemas operativos, ayudándonos de esta forma en el proceso de identificación de vulnerabilidades. A continuación mostramos algunas de las características de esta herramienta:

- Búsqueda de vulnerabilidades en la red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisión de actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

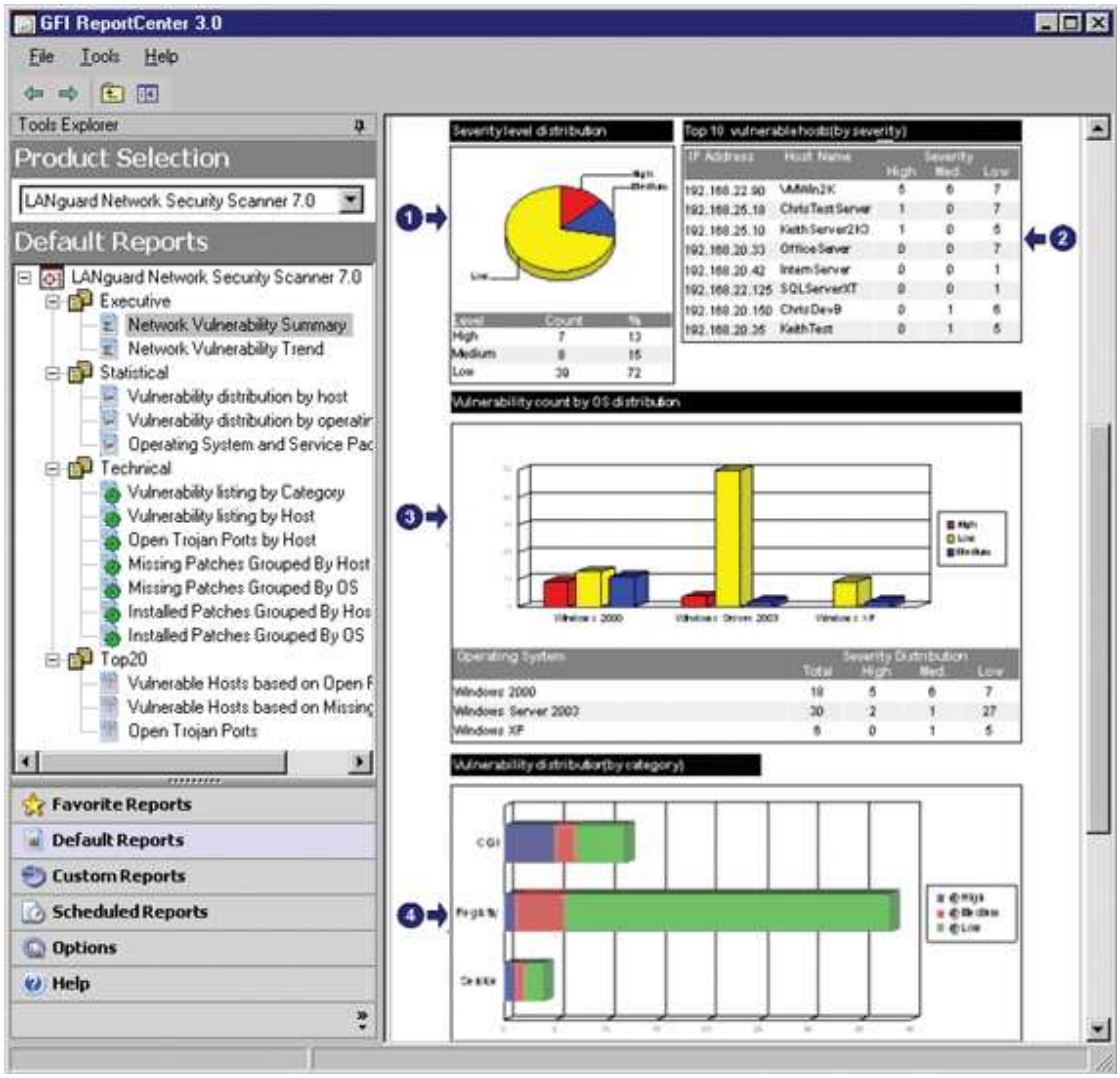


Figura 1.1. Herramienta de análisis de vulnerabilidades.

Fuente: Gfi languard publication

1.1.2.6 Análisis del impacto y el factor de riesgo

El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos:

Consecuencias de tipo económico, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de los Centros o Institutos de Instrucción Aeronáutica.
La importancia critica de los datos y el sistema (importancia a la organización).
Sensibilidad de los datos y el sistema.

1.1.2.7 Identificación de controles

En esta fase se evaluarán las conclusiones de la valoración respecto a la Norma ISO 27001:2005 y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

1.1.2.8 Plan de implementación tecnológica

El plan de Implementación tecnológica, se presenta como una herramienta para el control por parte de los Institutos Tecnológicos de Educación Aeronáutica de las actividades que se deben llevar a cabo para mitigar los riesgos identificados, en la evaluación de riesgo del proyecto en curso y de acuerdo al alcance definido.

La Seguridad de la Información, hoy en día se ha convertido como la carta de aeronavegavilidad para el tema de la inversión en tecnología, debemos en toda inversión tecnológica considerar aspectos relacionados con la Gestión de la Seguridad, con el fin de que esta inversión este alineada plenamente con la estrategia de estos Centros de Instrucción Aeronáutica y garantice de manera efectiva y eficiente su desenvolvimiento. Mas aún cuando estos Institutos ya empiecen a abrir su tecnología, hacia el uso sobre redes digitales de arquitectura abierta e inalámbricas para áreas extendidas.; pues la proyección y necesidad de capacitación es a nivel nacional , es decir en donde la operatividad aeronáutica requiera capacitación, y a corto plazo empiecen por establecer el uso de su actual tecnología de comunicaciones por satélites a fin de dar a conocer e implementar cursos o entrenamiento del sector aeronáutico para las áreas que las

especificaciones técnicas de la Dirección de Aviación Civil se lo permitan y que están detalladas en las RDAC 142, que es el instrumento legal que permite estos tipos de entrenamiento, básicamente de :

Formación de Técnicos en Operaciones de Vuelo
Formación de Observadores Meteorólogos Aeronáuticos
Formación de Controladores de Transito Aéreo
Formación de Técnicos en Telecomunicaciones Aeronáuticas
Formación de Bomberos Aeronáuticos
Formación de Auxiliares de Cabina.

1.2 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION

Para conocer los elementos que influyen en la seguridad. Se toma en consideración que los principios fundamentales de riesgo, que influyen en la seguridad de la información son la disponibilidad, la integridad y la confidencialidad. Los cuales previenen respectivamente: la interrupción de los servicios; la modificación no autorizada de sistemas e información; la revelación no autorizada de información sensitiva.

El primer grupo de requerimientos determinados son para analizar los riesgos que influirían en la **disponibilidad** y se demanda conocer lo siguiente:

- Si los Institutos disponen de un plan de continuidad; la existencia de una persona responsable del manejo y administración de una crisis; los procesos de recuperación y la puesta en funcionamiento de los sistemas.
- Si el plan de continuidad es el adecuado para efectuar una recuperación controlada de los sistemas, en un tiempo menor al considerado como crítico y si el plan es actualizado cada vez que se presenten cambios importantes en la infraestructura de los sistemas de información.
- Si el plan ha sido puesto a prueba en un ambiente de simulación de una situación crítica, y si se han detectado debilidades para efectuar los cambios necesarios para mejorarlo.
- Si se dispone de planes de contingencia para remediar problemas de dispositivos y servicios importantes, y si dispone de los medios de recuperación para salir de la crisis en un período de tiempo considerado aceptable.
- Si el Instituto tiene un grupo de personas responsables de poner en marcha los planes de contingencia, para habilitar los sistemas informáticos ante una catástrofe grave en la que esté afectada la infraestructura física, tal como: terremoto, incendio, inundación, acto terrorista.

- Sobre el riesgo de que los respaldos de la información no estén actualizados, y con los medios magnéticos guardados en sitios seguros fuera del área física del Instituto.
- El probable riesgo de que el personal responsable de la continuidad de la operación de los sistemas informáticos se ausente de manera provisional o definitiva; y las medidas que se aplican para garantizar la continuidad de las operaciones, tales como: duplicación y rotación de funciones, documentación de procedimientos, entrenamientos a doble comando.
- Si el Instituto es vulnerable a: incendio, inundación, explosión, mal funcionamiento del hardware de los equipos, fallas de energía, errores de aplicaciones (software), infecciones de virus informático, introducción de código malicioso.
- Sobre los riesgos que se relacionan con el control de acceso físico a las áreas que mantienen información sensitiva y confidencial, tales como: área de servidores, archivadores de medios magnéticos, etc.

El segundo grupo requerimientos es para analizar los riesgos que influyen en la **confidencialidad** de la información, y se solicita:

- Si existe riesgo de que personas no autorizadas observen información impresa en: los reportes enviados a impresoras ubicados en áreas públicas, copias impresas de correo electrónico, documentación con información confidencial, correspondencia, información que se escribe en tableros durante reuniones, archivadores, receptores de basura ubicados en sitios cercanos a equipos de destrucción de documentación, documentos transportados entre oficinas por medios físicos.
- La infraestructura física y organizacional del Instituto que puede afectar la confidencialidad del trabajo interno, tales como: la localización de las oficinas y centros de procesamiento de información, el tipo de separación entre oficinas, las características de puertas y ventanas, las facilidades de acceso que puede tener el personal ajeno al Instituto, el horario de ingreso al trabajo.

- Los controles de acceso físico para el ingreso a áreas que mantienen información sensitiva y confidencial, tales como: las áreas donde hay puntos de conexión a red, los documentos impresos, los monitores que despliegan información calificada.
- Los controles de acceso lógico para proteger la información y datos sensibles de personas no autorizadas, y los factores que influyen, tales como: el acceso a los sistemas vía red (enlaces en la Intranet, enlaces remotos vía telefónica, enlaces vía Internet), el uso de la red (periodicidad, tipos de datos transmitidos, características de la red, seguridad empleada), los mecanismos de autenticación empleados, la facilidad de acceso a las aplicaciones y recursos por medio de una estación de trabajo, el uso de técnicas de criptografía, los procedimientos de registro de eventos y auditoria, el procedimiento de diagnóstico de aplicaciones, la separación de los ambientes de producción y desarrollo.
- Lo relativo a la administración de los sistemas de información en las siguientes situaciones: el transporte de equipos entre oficinas, procesos que se utilizan cuando salen equipos de los Institutos para alguna reparación, la utilización de laptops por personal directivo fuera de las oficinas, los mecanismos que se utilizan para destrucción de material impreso conteniendo información calificada, los procedimientos de mantenimiento y actualización de hardware, los acuerdos de seguridad con los proveedores de equipos.
- Los riesgos que se relacionan con la estructura organizacional y la cultura de seguridad de quienes conforman el Instituto, si se dispone de políticas de seguridad confiables, si los auditores ofrecen un respaldo y son competentes, si existe un programa de concienciación de todos los niveles de funcionarios y estudiantes respecto a seguridad, si hay una actitud positiva del grupo responsable de seguridad, si en los procesos de contratación de personal esta considerado temas de seguridad, si existe un reglamento que sancione las faltas disciplinarias, y la existencia de políticas de asignación de responsabilidades.

La tercera parte de requisitos se relaciona con los riesgos que influyen sobre la **integridad**, se investiga:

- Los riesgos de que se produzcan errores en los siguientes casos: el ingreso de datos manualmente a través de teclado, la ejecución de procesos de revisión y reconciliación, los procesos de corrección y mantenimiento de bases de datos, los procesos de revisión de inventarios para conciliar datos, los procesos de verificación de entradas.
- Los riesgos por manipulación intencional y no autorizada de entrada de datos e información, por personas internas y externas a la organización.
- Los riesgos de que se produzcan errores por un mal funcionamiento de las aplicaciones (software), y que se pueden dar en las siguientes situaciones: cuando hay una falta de comunicación entre los ambientes de producción y desarrollo, el inadecuado control en los procesos de cambios en las aplicaciones, los cambios frecuentes y complejos, los requerimientos de cambios emergentes de las aplicaciones, la falta de experiencia del grupo de desarrollo, las presiones ejercidas para culminación de proyectos en tiempos establecidos, las aplicaciones muy complejas, las aplicaciones no estables, la no utilización de estándares, la carencia de control de calidad en el desarrollo, la falta de definición de los niveles de responsabilidad del grupo de desarrollo, la falta de controles de verificación y validación dentro de la aplicación, la ausencia de prácticas de auditoria, las malas prácticas de desarrollo.
- Los riesgos por la mala operación de los sistemas de información, debido a: la falta de experiencia y conocimiento de operadores, los permisos concedidos a los operadores se exageran, la falta de supervisión sobre las tareas de los operadores, la no revisión de registros de eventos, la falta de auditorias sobre el trabajo de los operadores, el desconocimiento de procesos.
- Sobre la existencia de planes para mitigar, administrar y recuperarse de algún incidente que afecte la integridad de la información.

1.2.1 RIESGOS IDENTIFICADOS QUE PODRIAN AFECTAR A LOS INSTITUTOS TECNOLOGICOS DE EDUCACION AERONAUTICA

RIESGOS DE ORIGEN FISICO

Catástrofes climáticas: Las zonas donde funcionan estos centros por lo general se ubican en ciudades que se encuentran expuestas a riesgos climáticos como: terremotos, inundaciones, grandes lluvias, tormentas eléctricas, erupción de volcanes (Pichincha y Cotopaxi).

Incendio: Puede afectar en forma directa a las instalaciones de sus centros de tecnología o en forma indirecta por humo, agua de los bomberos y escombros, si el incidente se produce en un lugar muy cercano.

RIESGOS DE ORIGEN TECNICO

Intrusión (Accesos no autorizados): Es cualquier acceso a la información confidencial de la Institución, por parte de una persona externa de forma no autorizada. Los riesgos principales de este tipo de acciones afectan la confidencialidad, pero una vez que el sistema ha sido penetrado pueden afectar la integridad y la disponibilidad de la información.

Ataques de virus: Si un virus infecta uno de los componentes de sus centros de tecnologías de información, puede quedar interrumpido uno o varios procesos críticos. Aunque los virus son desarrollados por personas, su disposición incontrolada y su funcionamiento hacen que se los considere como un riesgo técnico.

Spam: Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono celular.

Phising: Los intrusos pueden utilizar procesos consistentes en la suplantación de Identidad de la persona que llama (en el que se muestra una firma de ID de llamada falsa a los destinatarios) para cometer fraudes haciéndose pasar por

empleados de entidades en las que se confía con objeto de que los clientes divulguen información confidencial por ejemplo cuentas de usuarios, PIN y contraseñas.

Denegación de servicio DoS (Denial of Service): Se puede efectuar como producto de un ataque a una casilla de mensajes de voz, ya que podría ser inundada con mensajes de envío masivo y la línea podría ser interrumpida.

RIESGOS DE ORIGEN HUMANO

El enemigo interno malicioso: Se considera así al personal interno que busca venganza, beneficio económico y busca hacer daño en forma premeditada.

El enemigo interno inconsciente: Considerado aquel funcionario interno que actúa por negligencia, por inocencia y/o por ignorancia

Sabotaje: Es toda acción externa de daño directo o indirecto a cualquier parte del sistema Tecnología de Información y Comunicaciones con el objeto de afectar en principio su disponibilidad.

Hurto o robo: Un atacante que llegue a tener acceso a un servidor crítico de la Institución, podría ingresar a los datos almacenados, substraerlos y utilizarlos en propio beneficio. También se hace referencia al robo de dispositivos físicos del sistema, lo cual puede ser realizado por personas internas y externas de la Institución. El principal daño esta orientado a la disponibilidad del sistema.

Ingeniería social: Habrá el intento de obtener información calificada o sensible por medio de la palabra a un usuario autorizado del sistema, con el objeto de utilizar la información y superar las barreras de seguridad del sistema.

La disponibilidad debe ser garantizada mediante la preparación de planes de continuidad del negocio, y planes de contingencia. La responsabilidad de diseñar un plan de continuidad del negocio debe ser de involucramiento de todo el personal Directivo, Administrativo y toda la Institución como tal.

Para la ubicación de los servidores, se requiere de un área reservada donde se concentren los computadores principales y los dispositivos de comunicaciones, provistos de un aire acondicionado.

Por lo general no hay procesos establecidos para los respaldos de la información, y si los hay no son cumplidos en forma metódica algo culturalmente permanente.

La información que generan los usuarios en sus actividades diarias es generalmente almacenada en discos duros; varios de los mecanismos de estos dispositivos son electromecánicos y tienen un tiempo de vida útil. Los usuarios no efectúan los respaldos de información de una forma metódica y programada, por lo tanto, hay el riesgo de pérdida de información ante una eventual amenaza que afecte a un dispositivo de almacenamiento.

Es común que los integrantes de los departamentos o centros de tecnologías de esos Institutos, en corto tiempo adquieren un buen nivel de especialidad en el área, y se convierten en personas indispensables. El riesgo por ausentismo, puede generar una amenaza que afecte el normal desenvolvimiento del Instituto.

Todo avance tecnológico también trae consigo sus desventajas, e Internet no es la excepción. Las instituciones educativas en general están abiertas en su totalidad a la globalización, los Institutos de educación aeronáutica se relacionan con sus similares del mundo y por lo tanto tienen por lo menos un tipo de enlace hacia Internet. La falta de previsión y conocimiento ocasiona que no exista control sobre ciertas puertas lógicas, y esto da lugar a que personas extrañas puedan ingresar a los sistemas de información, y observen, modifiquen, y dañen la información. La falta de conocimiento trae consigo un exceso de confianza, que puede ser aprovechada por extraños para causar daños irreparables en la información.

1.2.1.1 Evaluación y tratamiento de los riesgos

Al analizar los resultados que se obtuvieron en la matriz de riesgos descrita, permitió clasificar a los riesgos según su prioridad, importancia, probabilidad de ocurrencia y el impacto que podrían ocasionar si uno de estos riesgos se materializara. Esta información será muy útil en el momento de tomar decisiones sobre el tratamiento de cada uno de los riesgos altos y medios identificados y las estrategias de emergencia y de recuperación.

Según el valor que obtenga cada uno de los riesgos se clasifican según el siguiente rango:

RIESGO	RANGO	
ALTO	8	10
MEDIO	4	7
BAJO	1	3

Tabla 2.1

Fuente: propia

1.2.1.2 Monitoreo

En los últimos años la tecnología ha crecido vertiginosamente y la gestión de riesgos va de la mano de esta evolución, por lo que es un proceso dinámico y precisa ser monitoreado y revisado periódicamente para procurar detectar cambios que pudieran afectar la eficiencia o costo- beneficio de los controles. El monitoreo deberá ser realizado permanentemente y revisado por lo menos cada 6 meses o 3 meses si así lo amerita.

1.2.2 IDENTIFICACION Y CLASIFICACIÓN DE LA INFORMACION EN SUS FORMAS Y MEDIOS DE ACUERDO A SU CRITICIDAD

DEFINICIONES

El objetivo de clasificar la información es organizarla de acuerdo a su sensibilidad a la pérdida y/o revelación de información. Cuando la información está clasificada de acuerdo a su nivel de sensibilidad, los directivos pueden decidir cuales controles de seguridad son necesarios para proteger los distintos tipos de información. Esto asegura que la información valiosa con un contenido importante, tenga un nivel de protección adecuado, mientras que la clasificación determina la prioridad de su aseguramiento. El propósito de la clasificación es indicar el nivel de confidencialidad, integridad y disponibilidad que es requerida para cada tipo de información.

La información adopta muchas formas, y puede ser: almacenada en los sistemas de información o en medios portables (Disquetes, CDs, flash memory, discos externos); transmitida a través de redes o entre sistemas de información; impresa o escrita en papel y o hablada en conversaciones.

Bajo el punto de vista de Seguridad, una protección adecuada debe ser aplicada a todas y cada una de las formas relacionadas con un Sistema de Información.

Previamente a su clasificación, debe realizarse un inventario de Activos de Información asociados a cada Sistema de Información.

TIPOS DE INFORMACIÓN

El Dueño de Datos deberá clasificar toda su información teniendo en cuenta la criticidad, prioridad y seguridad que sea necesaria.

La información se clasifica en los siguientes ítems:

INFORMACIÓN PÚBLICA

Toda aquella información que no representa riesgo significativo para la Institución y de acceso libre.

INFORMACIÓN RESTRINGIDA O DE USO INTERNO

Información que puede presentar riesgos para la Institución, y cuyo acceso debe ser expresamente autorizado por el Dueño de Datos y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales.

INFORMACIÓN CONFIDENCIAL

Toda aquella información de acceso autorizado que puede presentar riesgos importantes para la Institución, y que deben cumplir con las siguientes medidas adicionales de seguridad para limitar y proteger su uso:

Deben ser encriptados todos los archivos de datos sensibles tanto de producción como de cualquier otro ambiente en cualquiera de las siguientes situaciones:

- Procesamiento diario
- Conservación en los sistemas
- Transmisión electrónica a través de las redes
- Generación de copias de respaldo
- Conservación en logs de eventos

El Dueño de Datos correspondiente debe conservar toda información clave para la ejecución de los procesos de encripción y desencripción.

Para los reportes conteniendo información confidencial se deben utilizar impresoras dedicadas y de acceso físico restringido sólo a los usuarios autorizados.

Para la destrucción de los soportes impreso se deben utilizar trituradoras de papel.

No esta permitido su uso para propósitos de prueba en los desarrollos y/o implementaciones de sistemas, salvo expresa autorización del Dueño de Datos.

INFORMACIÓN SECRETA

Es la información que necesita tener los niveles máximos de protección de la información, ya que si es revelada a personas no autorizadas, puede ocasionar graves consecuencias para el dueño de datos y consecuentemente a la Institución.

A continuación en la tabla 2.2, se muestra la clasificación de la información, en la cual se encuentran las medidas de seguridad para cada tipo de información, los accesos autorizados y algunos ejemplos que pueden servir como guía.

TIPOS DE INFORMACION	MEDIDAS DE SEGURIDAD	ACCESOS	EJEMPLO
Pública	Mínimas	Público	Internet
Restringida o de uso interno	Normales	Personal Autorizado	Intranet
Confidencial	Especiales	Personal Autorizado específicamente	Presupuestos Recibo de Sueldos
Secreta	Extremas	Encriptadas solo sabe una persona	Contraseñas PIN

Tabla 2.2 Clasificación de la Información

Fuente: Manual de Políticas del ITSA

1.2.3 VINCULO DE LA CLASIFICACIÓN DE LA INFORMACIÓN CON LAS POLÍTICAS Y PROCEDIMIENTOS.

En un Instituto de Educación Aeronáutica se deben crear políticas que orienten como manejar los diferentes tipos de información; establecer las posibles amenazas y vulnerabilidades que afecten a los documentos; cuantificar las pérdidas que se pueden generar en la situación de que una amenaza se lleve a efecto, y determinar la manera de minimizar el impacto mediante una contramedida.

Luego se deben crear procedimientos que indiquen como ejecutar las políticas de clasificación de la información, tales como:

- Etiquetar la información luego que ha sido organizada y clasificada.
- Marcado de medios de almacenamiento como CDs, cartuchos, discos flexibles.
- Acuerdos con los empleados de no divulgación de información confidencial.
- Procesos de almacenamiento de información confidencial en lugares protegidos.
- Acceso restringido a lugares donde se imprima información reservada.
- Divulgación de información reservada solo debido a motivos de trabajo.
- Transmisión de información confidencial, por canales de comunicación que garanticen la seguridad de la información, utilizando técnicas digitales de encriptación.
- Procesos de transportación física de documentos reservados por medios confiables, y tomando preacusaciones ante posibles amenazas.
- Procedimientos de destrucción de documentos reservados, mediante la utilización de dispositivos diseñados para este propósito.

CAPITULO II

2 ELABORACION DE LA PROPUESTA DEL MODELO DE SGSI

INTRODUCCIÓN

En este capítulo se documenta la forma como proceder para realizar la construcción de la Propuesta de un Modelo de un Sistema de Gestión de Seguridad de la Información adaptado a los Institutos Superiores Tecnológicos de Educación Aeronáutica, basado en la serie de la Norma Internacional ISO 27000, investigación que fue posible realizarla en el ISTAC INSTITUTO SUPERIOR TECNOLOGICO DE AVIACION CIVIL, organización adscrita a la Dirección General de Aviación Civil,

2.1 ELABORACION DE LA PROPUESTA DEL MODELO DE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

2.1.1 TERMINOS Y DEFINICIONES

Un **SGSI** es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la Alta Dirección, para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

Un SGSI comprende la estructura organizativa, los procedimientos, los procesos y los recursos para implantar la gestión de la seguridad de la información.

El sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.)

Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.

2.1.2 APLICACIÓN DE LA NORMA ISO 27001: 2005

Debemos tener presente que:

Las medidas de seguridad deberán estar adaptadas a la estructura administrativa, al personal y al entorno tecnológico de cada uno de los Institutos Tecnológicos de

Educación Aeronáutica. El esfuerzo financiero y tecnológico deberá ser proporcional a los riesgos reales existentes."

La gestión de la seguridad de la información al interior de un Instituto Tecnológico de Educación Aeronáutica, esta enmarcada por los enunciados de las políticas de seguridad, encargadas de transmitir las decisiones administrativas del papel que desempeña la seguridad dentro de la Institución.

Las entrevistas iniciales y primeras aproximaciones en el ISTAC, complementadas con las encuestas para indagar los niveles de gestión de la seguridad de la información en el Instituto, permitieron observar limitaciones de aplicación de algunas políticas de seguridad planteadas por ellos de manera empírica , y en otras ninguna implementación debido a razones principalmente culturales, falta de conocimiento y una mala planificación para el establecimiento de sus reales necesidades económicas para la seguridad de la información. Así por ejemplo, se ve que no existe una política de seguridad que oriente al administrador y a los usuarios sobre los derechos de acceso, que pueden ser establecidos de manera individual o por grupo de trabajo, en función de un perfil o de determinada categoría de trabajo, definidas por distribución de roles y responsabilidades.

Otra realidad observada permite ver que no hay la tendencia a contratar consultorías externas para resolver problemas e implementar soluciones de gestión a la seguridad de la información. Dos son los motivos mencionados, las limitaciones económicas y el celo profesional del administrador para no ser desplazado de su función.

La falta de gestión ocasiona que no se realicen auditorias de las aplicaciones ha donde ingresan los usuarios y la información a la cual acceden, con el fin de hacer evaluaciones e imponer correctivos si el análisis así lo determina.

En conclusión, se ha observado que en este Instituto, no es prioridad el operativizar la seguridad de la información, por tal motivo las políticas de seguridad que deben estar documentadas no existe. A lo que se suma la falta de apoyo económico, de los principales auspiciantes de la Dirección de Aviación Civil.

Vemos entonces que las políticas, procedimientos y guías de seguridad, son elementos dinámicos que deben modificarse de acuerdo a los cambios organizacionales de estos Institutos y a las innovaciones tecnológicas en seguridad de la información; al igual que a los cambios del entorno político, social y económico del país.

Los planteamientos de Gestión de Seguridad de la información, resumidos por medio de políticas, serán válidos por un determinado periodo de tiempo. Los enunciados de las políticas cumplen una permanencia limitada, luego de lo cual será necesario actualizarlas y por tanto se crearán nuevas adaptaciones; por lo expuesto es necesario contar con un Modelo que estructure, organice y defina adecuadamente estos procesos de cambio.

Según expertos un certificado ISO 27001 demuestra que un Sistema de Gestión de Seguridad de la Información ha sido certificado bajo una norma de acuerdo a las buenas prácticas. Cuando una entidad de certificación ha expedido el certificado demuestra que ha tomado suficientes precauciones para proteger la información confidencial contra el acceso no autorizado y los cambios.

La norma adopta un proceso (PDCA) enfocado para **establecer, implantar, funcionar, seguir, revisar, mantener** y **mejorar** un Sistema de Gestión de la Seguridad de la Información de cualquier tipo de organización, es por lo tanto adaptable a este tipo de institutos, relativamente pequeños.

La norma sigue un enfoque detallado hacia la seguridad de la información. Activos que necesitan un ámbito de protección desde información digital, documentos en papel, y activos físicos (ordenadores y redes) para el conocimiento de cada

empleado. Cuestiones que hay que abordar desde el desarrollo de competencia del personal hasta la protección técnica contra el fraude informático.

ISO/IEC 27001 permite proteger la información en términos de:

- Asegurar la **confidencialidad**, que la información está accesible solo para aquellas personas autorizadas a tener acceso.
- Proteger la **integridad** de la precisión y totalidad de la información y los métodos de tratamiento.
- Garantizar la **disponibilidad**, que los usuarios autorizados tengan acceso a la información y los activos relacionados cuando lo necesitan.

El objetivo último es llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA y el proceso de mejora continua comunes a todos estos estándares. Las facilidades para la integración de las normas ISO 27000 son evidentes mediante la consulta de sus anexos.

2.1.3 LA SERIE 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO 27000**: En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tienen un costo.

- **ISO 27001**: Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 la misma que ha sido mejorada, ante la cual se certifican los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En el Anexo A de la norma, se enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online. Otros países donde también está publicada en español son, Colombia, Venezuela y Argentina. El original se encuentra escrito en inglés y tiene un costo de $ 200, oo dólares.
- **ISO 27002**: Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original esta escrito en inglés.
- **ISO 27003**: En fase de desarrollo; su fecha prevista de publicación es mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos

publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO 27004**: En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.
- **ISO 27005**: Publicada el 4 de junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.Esta norma aún no está traducida.
- **ISO 27006**: Publicada el 13 de febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoria y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. Todavía no se encuentra traducida al español.
- **ISO 27007**: En fase de desarrollo; su fecha prevista de publicación es mayo de 2010. Consistirá en una guía de auditoria de un SGSI.

- **ISO 27011**: En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).
- **ISO 27031**: En fase de desarrollo; su fecha prevista de publicación es mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- **ISO 27032**: En fase de desarrollo; su fecha prevista de publicación es febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.
- **ISO 27033**: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028.
- **ISO 27034**: En fase de desarrollo; su fecha prevista de publicación es febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.
- ISO **27799**: Publicada el 12 de junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números,

grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida. El original se encuentra en inglés

2.1.4 PROPUESTA DEL MODELO SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI

2.1.4.1 ALCANCE

Se cubre todos los 39 objetivos de control listados en las secciones 5 a 15 de ISO/IEC 27002, además de la sección 4 de evaluación y tratamiento de riesgos que les precede.
Los objetivos de control y controles deben seleccionarse como parte del proceso SGSI especificado en la sección 4.2.1 de la Norma ISO 27001:2005

2.1.4.2 OBJETIVO DE LA PROPUESTA

Constituirse en un documento genérico que permita, implantar el estándar ISO de Gestión de Seguridad de la Información adaptado a la Norma de la serie 27000

2.1.4.3 PASOS PREVIOS

COMPROMISO DE LA DIRECCIÓN:
Una de las bases fundamentales para iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección del Instituto. No sólo por ser un punto contemplado

de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.

PLANIFICACIÓN, FECHAS, RESPONSABLES:
Como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases, por tanto es aconsejable definir las fechas y quienes participarán.

2.1.4.4 DESARROLLO DEL MODELO

Debemos seguir los siguientes pasos, referenciados a la serie ISO 27000 que nos permiten medir y reportar el estado de la seguridad de la información de la siguiente forma:

Ref.	Objetivo	Consejos de implementación	Posibles métricas
4. Evaluación y tratamiento de riesgos			
4.1	Evaluación de riesgos de seguridad	Se puede usar cualquier método de gestión de riesgos de seguridad de la información, con preferencia por métodos documentados, estructurados y generalmente aceptados como OCTAVE, MEHARI, ISO TR 13335 ó (y, en su momento, ISO/IEC 27005).	Porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".
4.2	Tratamiento de riesgos de seguridad	La Dirección (específicamente, los propietarios de activos de información) necesita evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones	Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia. Costos de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		deben documentarse en un Plan de Tratamiento de Riesgos (PTR). Es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información que se estiman dentro de la "tolerancia al riesgo" de la organización, sin que sea éste el enfoque comúnmente aceptado.	Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios.
5. Política de seguridad			
5.1	Política de seguridad de la información	Establecer el Manual de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoria, gerencia o auto-evaluación).
6. Aspectos organizativos de la seguridad de la información			

Ref.	Objetivo	Consejos de implementación	Posibles métricas
6.1	Organización interna	Establecer la estructura y tamaño de otras funciones corporativas especializadas, como Secciones: legal, Riesgos y Auditoria.	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.
6.2	Terceros	Haga inventario de conexiones de red y flujos de información significativos con 3as partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos. Esto puede causar temor, pero es 100% necesario Considere exigir certificados en ISO/IEC 27001 a los *partners* más críticos, tales como *outsourcing* de TI, proveedores de servicios de seguridad TI, etc.	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.
7. Gestión de activos			
7.1	Responsabilidad sobre los activos	Elabore y mantenga un inventario de activos de información (similar al preparado en su día para el *Efecto 2000*), mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. ej.,	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.). Use en lo posible códigos de barras o similares para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.	dichos riesgos en niveles aceptables.
7.2	Clasificación de la información	Mantener el principio de simplicidad.Distingir los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo. Es práctico comenzar por la confidencialidad, pero sin descuidar los requisitos de integridad y disponibilidad.	Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").
8. Seguridad ligada a los recursos humanos			
8.1	Antes de la contratación	Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación,	Porcentaje de nuevos empleados, aspirantes o similares (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas del Instituto antes de comenzar a trabajar.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		conocimientos, etc.	
8.2	Durante la contratación	La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegurar que esto se documente claramente en materiales de concienciación, contratos de empleo, etc. Contemplar la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.	Respuesta a las actividades de concienciación en seguridad medidas por, p. ej., el número de e-mails y llamadas relativas a iniciativas de concienciación individuales.
8.3	Finalización laboral o cambio de puesto de trabajo	Revisar la Sección 7.1. La devolución de los activos de la organización cuando un empleado termina su relación laboral sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Determine y establezca qué accesos necesita revocar en primer lugar cuando un funcionario presenta su renuncia: ¿cuáles son los sistemas más críticos o vulnerables? Haga un seguimiento del uso del e-mail por estas	Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		personas antes de salir definitivamente de la Institución, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).	
9. Seguridad física y ambiental			
9.1	Áreas seguras	El estándar parece centrarse en el Centro de Computo, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examinar los procedimientos de entrada y salida de personas ajenas a la Institución. Ejemplo ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Usar tarjetas de identificación, similares a las Tarjetas de circulación	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		aeroportuaria distinguibles por colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la Sección Tranair, verde para el Dpto. Académico, etc.; Establezca la políticas a seguir con los intrusos sin identificación Asegurarse de poner en práctica las políticas de retirar todos los pases de acceso de funcionarios y de visitantes cuando se vayan. Hacer que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Disponer la utilización de pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las 24 horas de haberse emitido.	
9.2	Seguridad de los equipos	Promover que el sistema de vigilancia privada contratado o propio, impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos de TI, de las instalaciones sin autorización escrita. Conviértalo en un procedimiento disuasivo visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Estar especialmente atento a puertas traseras,	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		rampas de carga, salidas para fumadores, etc. Tomar en cuenta el uso de códigos de barras para hacer los chequeos más eficientes.	
10. Gestión de comunicaciones y operaciones			
10.1	Responsabilidades y procedimientos de operación	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de políticas de seguridad de la organización.	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-).
10.2	Gestión de la provisión de servicios por terceros	¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema de supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio. Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. En algunos casos puede funcionar un sistema de premio y castigo. Esté atento a cambios que	Costo del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		tengan impacto en la seguridad.	
10.3	Planificación y aceptación del sistema	Adoptar procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, etc., usando estándares aceptados como ISO 20000 (ITIL) donde sea posible. Defina e imponga estándares de seguridad básica (mínimos aceptables) para todas las plataformas de sistemas operativos, usando las recomendaciones de seguridad de CIS, NIST, NSA y fabricantes de sistemas operativos y, por supuesto, sus propias políticas de seguridad de la información.	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similares y (b) cuya conformidad con dichos estándares ha sido comprobada mediante *benchmarking* o pruebas.
10.4	Protección contra código malicioso y móvil	Combinar controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación). De nada sirve tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables	Tendencia en el número de virus, gusanos, troyanos o *spam* detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.
10.5	Copias de seguridad	Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de	Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba exitosas. Tiempo medio transcurrido desde la

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		negocio "internos" de la Institución. Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes. Encripte copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?).	recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.
10.6	Gestión de la seguridad de las redes	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
10.7	Manejo de los soportes	Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Encripte todos los datos sensibles o valiosos antes de ser transportados.	Porcentaje de soportes de backup o archivo que están totalmente encriptados.
10.8	Intercambio de información	Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones *offline* por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.
10.9	Servicios de intercambio electrónico	Trabaje estrechamente con las unidades de académicas para desarrollar un e-learning seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de eCommerce, desde el principio (también en cualquier cambio/actualización posterior). Insista en el valor agregado de la seguridad en la reducción de riesgos comerciales, legales y operativos asociados al	Estadísticas e informes sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas, cambios planificados, etc.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		eBusiness. Trabaje los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad. Determinar políticas claras para el uso seguro de los sistemas académico y portal institucional cuidando la inviolabilidad a las áreas sensibles de Admisión y Registro, Finanzas,	
10.10	Supervisión	El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico. Analice la criticidad e importancia de los datos que va a monitorear y cómo esto afecta a los objetivos globales de negocio de la Institución en relación a la seguridad de la información.	Porcentaje de sistemas cuyos *logs* de seguridad (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de *logs* y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los *logs* de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.
11. Control de accesos			
11.1	Requisitos de funcionalidad para	Los propietarios de	Porcentaje de sistemas y aplicaciones corporativas para los que los

Ref.	Objetivo	Consejos de implementación	Posibles métricas
	el control de accesos	activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de responsabilizar los incumplimientos, no conformidades y otros incidentes.	"propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.
11.2	Gestión de acceso de usuario	Crear la función especializada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y el Departamento de Seguridad de la Información. Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible.	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier variación (p. ej., "Implantada nueva aplicación financiera este mes").

Ref.	Objetivo	Consejos de implementación	Posibles métricas
11.3	Responsabilidades del usuario	Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentada y (b) formalmente aceptada.
11.4	Control de acceso a la red	Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).	Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas Web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).
11.5	Control de acceso al sistema operativo	Implante estándares de seguridad básica para todas las plataformas informáticas y de comunicaciones, recogiendo las mejores prácticas de CIS, NIST,	Estadísticas de vulnerabilidad de sistemas y redes, como numero de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias).

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		fabricantes de sistemas, etc.	
11.6	Control de acceso a la aplicación y a la información	Implante estándares de seguridad básica para todas las aplicaciones y middleware, recogiendo las mejores prácticas y checklists de CIS, NIST, fabricantes de software, *etc*.	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)".
11.7	Ordenadores portátiles y tele trabajo	Establecer políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware. Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.	Estado de la seguridad en entorno portátil / tele trabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, PDAs, teléfonos móviles, etc.), y de tele trabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, firewalls personales, etc.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
12. Adquisición, desarrollo y mantenimiento de los sistemas de información			
12.1	Requisitos de seguridad de los sistemas de información	Involucre a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan. Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien. Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas. Numerosas referencias ofrecen orientación sobre la implementación, como, p. ej., OWASP.	Ver 11.1

Ref.	Objetivo	Consejos de implementación	Posibles métricas
12.2	Procesamiento correcto en las aplicaciones	Siempre que sea posible, utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc. Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control). Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc.	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.
12.3	Controles criptográficos	Utilice estándares formales actuales tales como AES, en lugar de algoritmos de cosecha propia. La implementación es crucial	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses).
12.4	Seguridad de los archivos de sistema	Aplique consistentemente estándares de seguridad básica, asegurando que se siguen las recomendaciones de CIS, NIST, fabricantes de sistemas, etc.	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
12.5	Seguridad en los procesos de desarrollo y soporte	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.
12.6	Gestión de la vulnerabilidad técnica	Haga un seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update o Secunia Software Inspector.) Evalúe la relevancia y criticidad o urgencia de los parches en su entorno tecnológico. Pruebe y aplique los parches críticos, o tome	Latencia de parcheo o semiperiodo de despliegue (tiempo que ha llevado parchear la mitad de los sistemas vulnerables -evita variaciones circunstanciales debidas a retrasos en unos pocos sistemas, tales como portátiles fuera de la empresa o almacenados-).

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente. Evite quedarse tan atrás en la rutina de actualización de versiones que sus sistemas queden fuera de soporte por el fabricante.	
13. Gestión de incidentes en la seguridad de la información			
13.1	Notificación de eventos y puntos débiles de la seguridad de la información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad.	Estadísticas del *helpdesk* de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
13.2	Gestión de incidentes de seguridad de la información y mejoras	Las revisiones post-incidente y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.	Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida. Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.
14. Gestión de la continuidad del negocio			

Ref.	Objetivo	Consejos de implementación	Posibles métricas
14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.). Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio. Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre. Obtenga consejos de implantación en Gestión de la Continuidad de Negocio.	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante tests apropiados en los últimos 12 meses.
15. Cumplimiento			

Ref.	Objetivo	Consejos de implementación	Posibles métricas
15.1	Cumplimiento de los requisitos legales	Obtener asesoramiento legal competente, especialmente si la Institución opera o tiene reracionamiento en múltiples jurisdicciones.	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorias objetivas o de otra forma admisible, han sido considerados conformes.
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.	Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.
15.3	Consideraciones de las auditorias de los sistemas de información	Invierta en auditoria TI cualificada que utilice ISO 27001, CobiT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación. Examine ISO 19011 "Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiental" como fuente valiosa para la realización de auditorias internas del SGSI. ISO 19011 proporciona un marco excelente para crear un programa de	Número de cuestiones o recomendaciones de auditoria, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de hallazgos de auditoria relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorias.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
		auditorias internas y contiene asimismo las calificaciones del equipo de auditoria interna.	

2.1.4.5 CONSEJOS PRACTICOS

- Mantener permanentemente el principio de simplicidad y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.

- Comprender en detalle el proceso de implantación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.

- Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.

- Utilizar como guía una Estructura Desglosada de Trabajo WBS.(Work Breakdown Structured)

- La autoridad y compromiso decidido de la Dirección del Instituto -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.

- La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.

- No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.

- Servirse de lo ya implementado: otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.

- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.

- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

2.2 REQUERIMIENTOS DE IMPLANTACION DEL SISTEMA DE SEGURIDAD DE INFORMACION

Una adecuada implantación de este Modelo requiere, se rompan esas diferentes barreras de orden cultural principalmente que afectan a nuestro entorno social, que es el que define nuestra forma de pensar respecto a la adopción o no de nuevos instrumentos como este que nos obligan a enrumbarnos hacia las prácticas de los países desarrollados en implementar estos modelos. La educación superior y en particular de los centros de instrucción aeronáutica se desenvuelve en un clima de competitividad, cada centro educativo trata de innovar y ponerse a la vanguardia, mas por motivaciones de orden económico, pues en la

actualidad en el país la educación superior se ha convertido en una forma de lucrar, mas no de servir; esto hace que cada vez mas aparezcan nuevos centros de enseñanza en general, la creación de universidades ha proliferado últimamente, ofreciendo carreras similares en el ámbito aeronáutico una de ellas es por ejemplo la Universidad San Francisco, que ha creado la carrera de ciencias aeronáuticas, pero a costos realmente fuera del alcance del sector de la clase media.

Institutos como el ISTAC, ITSA, tienen potenciales fuentes de crecimiento y expansión, pues poseen uno de los principales activos de información que impulsaría este propósito, el cual es su conocimiento sobre la rama especifica del sector aeronáutico, es decir su Know how que en otras palabras es la sinergia de su experiencia. Este se convierte por tanto en uno de sus principales activos a proteger.

Poco a poco va consolidándose entre los usuarios de las nuevas tecnologías (y sobre todo Internet) la idea de que la seguridad no es una característica optativa de los sistemas y aplicaciones que utilizan; opinan que los sistemas deben ser seguros para que puedan confiar razonablemente en ellos antes de usarlos.
Y esa misma idea también tiene que ir cuajando entre los responsables de la gestión de los sistemas de información: la seguridad ya no es una opción; no solo es necesaria, sino que en muchos casos es, obligación.

Como resultado de esta nueva situación, la implantación de este Modelo de SGSI, promueve la satisfacción de por lo menos los siguientes requerimientos:

2.2.1 INVOLUCRAMIENTO DE LA ALTA DIRECCION

El apoyo permanente del ámbito directivo, se constituye en uno de los principales requerimientos para su implantación, su participación en el proyecto es de vital importancia, ya que el entendimiento claro y apoyo a la gestión del Jefe de

Proyecto o persona que se encuentre implementando este Sistema marcará la ruta por la cual se encamine el proceso de implementación. Además que implica que el cumplimiento posterior de las políticas que se establezcan se traduzca en disposiciones para todos los niveles de estas organizaciones de la rama educativa aeronáutica.

El Director o el que ocupe las altas direcciones, serán los que promuevan el desarrollo de la organización existente, por tanto la continuidad esta dada en función de su pensamiento de desarrollo institucional.

Su participación también definida en la Planificación Estratégica Institucional, incluirá el desarrollo de las TIC en la competitividad educacional; ya que hoy en día, las TIC deben responder a las necesidades de los negocios y el sentido de negocio en el área aeronáutica va mas allá de las expectativas inmediatas, pues el rumbo de la educación aeronáutica definirá el desarrollo aeronáutico del país. Es pues entonces claro que como utilizo la información es lo que me agrega valor.

2.2.2 EQUIPO DE IMPLANTADORES (STAKEHOLDERS)

El trabajo en equipo, en todo tipo de proyecto, se llega a constituir en el éxito del proyecto, en las TIC la combinación creativa de la gente e información es lo que produce resultados de excelencia. Para que un equipo de implantadores de un SGSI, tenga resultados se debe contar por lo menos con el siguiente equipo.

2.2.2.1 Definición de roles y responsabilidades

a) Un líder o Jefe de Proyecto, que es quien dirige el proceso de implantación

b) Un Patrocinador, que en muchos de los casos debería ser el mismo Director del Instituto, y es quien avaliza el seguimiento del proceso de implantación en conjunto con el líder del proyecto.
c) Un administrador , que en si se constituye el oficial de seguridad, y es quien realmente es el responsable de la implantación y seguimiento continuo de todo el proceso denominado PDCA, es decir de planear, implementar, monitorear, y mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
d) Los Propietarios de la Información, que es todo el personal que mantiene y retiene en si la autorización por el manejo de la información en todo el ciclo del proceso.
e) El Personal de Auditoria Interna y Externa, quienes efectuarán el control
f) Los usuarios, el personal de sistemas y terceros, que prácticamente son los involucrados en el cumplimiento de la normatividad, vía políticas, establecida para el Instituto.

2.2.3 SOFTWARE

Durante el desarrollo de esta tesis, hemos podido observar que se tornaría más dinámico el trabajo de planeamiento e implementación cuando se pueda contar con herramientas informáticas, que permitan agilitar estos procesos. A continuación mencionamos los paquetes informáticos, su uso y aplicación y donde ubicar una versión trial

APLICACION	UTILIDAD	DIRECCION
WBS	Elaboración de una forma estructurada el trabajo de planeamiento y/o implementación	www.criticaltool.com
GFI LANGUARD	Detección de vulnerabilidades	www.gfi.com

2.2.4 MANTENIMIENTO Y ADMINISTRACION

La política de seguridad genérica, resultante de este Modelo se debe redactar con la intención de que sea válida durante un período aproximado de unos cuatro años (si no se producen grandes cambios en la organización que obliguen a lo contrario); sin embargo, los procedimientos operativos que le dan soporte y la concretan deben mantenerse permanentemente actualizados, para reflejar siempre la realidad del sistema. Debe establecerse el período de revisión de cada procedimiento operativo, dejándolo abierto a revisiones extraordinarias motivadas por una necesidad de mejora. Aplicar el Principio del Kaizen, es decir mejorar lo mejorado.

Otro mecanismo de gran importancia -por su carácter totalmente práctico- para el mantenimiento de las medidas de protección implantadas y que, sin embargo, es olvidado con frecuencia, son los ensayos: de planes de contingencia, de recuperación de copias de respaldo de datos, y de respuesta a incidentes de seguridad.

Y no debe olvidarse el primero de los factores de éxito para el mantenimiento del Sistema de Gestión de Seguridad de la Información implantado: la prevención. Que puede concretarse en acciones como: la recolección, análisis y revisión de los registros de actividad (logs), la atención a un servicio que nos avise de las vulnerabilidades detectadas en las aplicaciones y equipos de nuestro sistema, y la reconfiguración de equipos HW, herramientas SW y, en el límite, de la arquitectura de la red (ubicación de los proxys, etc.), atendiendo a los avisos de vulnerabilidades recibidos -para así evitar los riesgos asociados-.

2.2.5 DISPONIBILIDAD 24X7

Los usuarios, llámese estudiantes, personal administrativo, etc, etc., aspirarán a que el Sistema de Gestión, este disponible siempre, esto es las 24 horas del día los 7 días de la semana.

Cuando se ofrece un servicio con altos requisitos de disponibilidad debe plantearse la necesidad de reestablecer de inmediato el Sistema.En este caso la políticas determinaran la calidad de este servicio

2.2.6 REGLAMENTACIONES O DISPOSICION LEGALES

Hay que recordar que una buena gestión, no es posible sin una buena reglamentación, o dicho de otra manera es la legislación interna y externa lo que determina que la aplicabilidad del Sistema tenga sustento para su fiel cumplimiento en la fase de implementación.

Se dice en términos comunes que la gente no hace lo que se dice que haga, sino lo que se le controla y supervisa, por tanto un mecanismo con el que se puede exigir o supervisar las existencia de reglamentaciones y/o disposiciones que cuenten con la firma y aval del Director.

2.2.7 SOCIALIZACIÓN DEL MODELO

Se concluye con este requerimiento ya que es uno de los más importantes, como paso previo a su implementación. Es necesario que todos los involucrados conozcan el que y para que de este SGSI, la socialización en base de charlas inductivas, marketing interno en la Institución, incentivos de participación y concienciación de la utilidad de este sistema como una herramienta de Gestión Integral. Cabría la necesidad de indicar que la regla de Pareto en esta parte tiene una aplicación casi real, ya que si dedicamos un 20 % de la fase de implementación del Modelo a indicar su real validez, significado, utilidad y aplicabilidad, obtendremos el 80 % de la comprensión y participación de todos los involucrados en este proceso.

2.2.7.1 Establecimiento de las políticas de seguridad

El objetivo es establecer las políticas de seguridad de la información

Se debe comenzar por establecer el Manual de Políticas de Seguridad de la Información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices.

El propósito de una política de seguridad es informar a los usuarios, personal del área de sistemas, jefes de Departamento, Alta Dirección, de su obligación de proteger los bienes informáticos; la política determina los mecanismos que son establecidos para proteger los valores de confidencialidad, disponibilidad e integridad.

Las políticas de seguridad deben desarrollarse como un esfuerzo conjunto entre el personal técnico, que comprenderá las implicaciones de implementar las diversas propuestas, y de los directivos los cuales deciden destinar los recursos necesarios para ejecutar la política en sí.

Todas las personas de la organización deben conocer su nivel de responsabilidad en la seguridad de la información. La política de seguridad no puede anticipar todas las posibilidades, pero si asegurar que para cada tipo de problema hay alguien asignado como responsable del mismo.

CAPITULO III

3 EVALUACION DE LA APLICABILIDAD DE LA PROPUESTA

En este capitulo se realiza la evaluación de la aplicabilidad de la Propuesta de Modelo de Gestión de Seguridad de Información, basados en el Instituto Superior Tecnológico de Aviación Civil.

3.1 EN EL ASPECTO LEGAL

Para el caso de la evaluación de la aplicabilidad en el aspecto legal debemos primero mencionar que al ISTAC lo rigen las siguientes leyes y reglamentos:

Ley Orgánica de Educación Superior
Ley de Aviación Civil
Regulaciones Técnicas de Aviación Civil (RDAC)
Reglamento General de Institutos Superiores Técnicos y Tecnológicos
Reglamento Interno.

De los controles detallados en la ISO/IEC 27001-2 cabe destacar el relativo a la revisión de los aspectos legales y contractuales que sean de aplicación y relevancia a cada sistema de información. El objetivo de esta revisión legal es doble:

- Evitar los incumplimientos de cualquier norma, reglamento, regulación u obligación contractual que sea de aplicación.

- Diseñar, operar, usar y gestionar los Sistemas de Gestión de la Información de conformidad con las exigencias legales, reglamentarias y contractuales que sean de aplicación.

El primer aspecto del control legal a tomar en consideración es llevar a cabo la identificación de la legislación aplicable al sistema de gestión de seguridad de la información que vaya a ser objeto de control, en este caso lo mencionados en el primer párrafo. A su vez hay que distinguir entre:

- Aspectos jurídicos específicos del tipo de actividad en que se encuadra cada organización. Este caso es el sector Educativo Aeronáutico
- Aspectos jurídicos comunes a todo tipo de organización.

El segundo aspecto del control legal a tomar en consideración es la revisión del cumplimiento de la legislación identificada, sobre la base de unos criterios previamente definidos, en función del alcance que se pretenda dar a la revisión de los aspectos legales. Es decir, un “traje a medida” garantizando siempre unos mínimos.
En particular, de los aspectos jurídicos comunes a todo tipo de organización, la ISO/IEC 27002 identifica, de modo meramente enunciativo, los siguientes:

- Propiedad Intelectual.

- Protección de Datos de carácter personal.

- Uso de las herramientas tecnológicas por parte de los usuarios de los sistemas de información de la organización.

- Registros de información de la organización.

- Medios y procedimientos de preconstitución de medios de prueba.

- Reglamentación de los controles de cifrado y uso de firma electrónica.

Ahora bien, un rasgo que caracteriza a la ISO/IEC 27002 es el hecho de que la misma no es certificable; es decir, no nace con la voluntad de ser imperativa ni vinculante, sino más bien como una “guía práctica” donde se detallan unos controles y pautas que puedan ser observadas de forma voluntaria.
Es por ello que se puede percibir que la aplicabilidad de este Modelo cumple y se ajusta a la normatividad actual del ISTAC, y no solo de el sino de los demás

Institutos de Educación Aeronáutica, ya que si por una parte, la guía de buenas practicas que hemos recogido de la ISO 27002, no es certificable, por otra en cambio toma la relación de controles que se deberán evaluar y considerar para establecer un SGSI basados en la ISO 27001 que si es CERTIFICABLE. Por tanto este modelo es una forma de contribuir a reducir, en la medida de lo posible, los riesgos de los sistemas de información de los Institutos Superiores Tecnológicos de Educación Aeronáutica a través de una gestión eficaz de los procesos de seguridad y, consecuentemente, una forma de avanzar en el camino de la excelencia educativa. Y un buen SGSI exige, ante todo, gestionar. Esto es, administrar, redactar políticas, normas y procedimientos, implantarlos y verificar su cumplimiento, siendo un proceso continuo que debe ser controlado, gestionado y monitorizado.

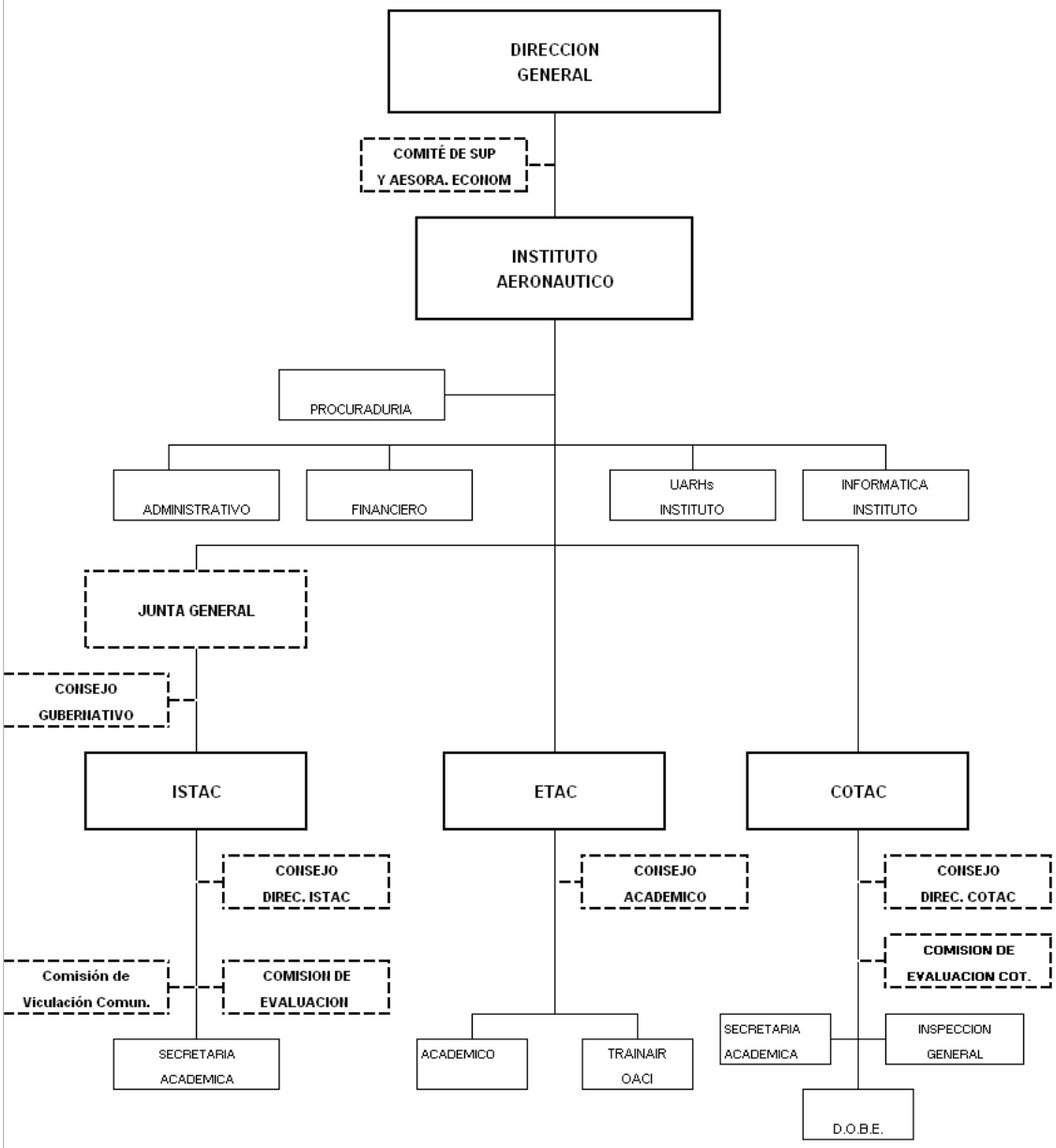
3.2 EN EL ASPECTO ORGANIZACIONAL

La actual estructura organizacional del ISTAC es la siguiente:

DIRECCION GENERAL DE AVIACION CIVIL

ESTRUCTURA DEL

INSTITUTO AERONAUTICO



La norma ISO 27001, claramente señala que: la adopción de un SGSI, debe ser decisión estratégica de la organización, y que el diseño e implementación del mismo es influenciado por las necesidades y objetivos, requerimientos de seguridad , los procesos empleados y lógicamente el tamaño y estructura de la organización, por lo que respecto a la actual estructura organizacional del ISTAC, el modelo que nos ocupa es aceptablemente adecuado ya que incluso no existe ninguna aplicación reglamentada, disposición o una subdivisión de la organización que apliquen en materia de Seguridad de la Información algo formal y establecido orgánica y legalmente para su implementación, únicamente se dispone de controles y políticas aisladas.

Es importante señalar que, la alta dirección de este instituto, ha dispuesto la implementación de una nueva estructura organizacional basada en una estructura por procesos, la misma que se detalla a continuación:

De la misma forma, la norma es también previsiva en cuanto a estos cambios pues, se adelanta y prevé futuros cambios, y que la implantación también se extienda en concordancia con las necesidades de las organizaciones.

Debemos señalar si de lo observado que en si el Modelo permitirá incrementar el compromiso interno, dado que la utilización de una norma de reconocida certificación que sustenta el SGSI, permitirá garantizar la eficacia de los esfuerzos desarrollados en materia de Gestión de Seguridad de la Información en todos los niveles de la organización, aún en la estructura proyectizada a implementarse en pocos meses.

3.3 EN EL ASPECTO OPERACIONAL

El Instituto Tecnológico de Aviación Civil ISTAC , es una entidad dependiente de la Dirección General de Aviación Civil; en este sentido, la División de Estándares de Vuelo de este organismo ha otorgado a este instituto ciertas normativas especiales, denominadas “Especificaciones Técnicas de Entrenamiento” que le permiten tener la Certificación de Centro de Instrucción Aeronáutico y que se constituyen en mecanismos legales para operativizar el trabajo de estos centros, así mismo Organismos como la Organización de Aviación Civil Internacional OACI, lo han Certificado como Centro de entrenamiento regional para Centro y Sud América, estas dos consideraciones se constituyen en el insumo de requerimientos y expectativas de su seguridad de información en su diario convivir, lo que operativiza mas aún la implementación de nuestro modelo, ya que el solo hecho de tener una metodología ordenada, similar a una lista de chequeos o check list, para la observación al detalle y cumplimiento de qué hacer en materia de Gestionar la Seguridad en esta rama del conocimiento especifico del entrenamiento aeronáutico promueve una aplicabilidad a sus actuales necesidades.

Por otra parte para que en el aspecto operacional se pueda llegar a implementar totalmente el Modelo siempre será necesario la participación de todos los involucrados, mas que su conocimiento especifico en el área tecnológica, es su deseo de compromiso con la Seguridad de la Información de su Instituto, ya que nuestro modelo es mas que una propuesta, es un modelo de planificación y como toda planificación siempre pone el mejor escenario para poder llegar a algo deseado, partiendo de una línea de base.

Así mismo es necesario subrayar que siempre es indispensable realizar una adecuada gestión de la documentación para que todos los procesos de implementación tomen forma y se operativicen finalmente mediante las firmas de responsabilidad, o dicho de otra manera la oficialización de las políticas, procedimientos, normas y demás aspectos que operativicen la Gestión de la Seguridad de la Información, tiene su validez mediante las firmas de los responsables en cada uno de los procesos o fases de implementación.
La aplicabilidad del modelo en el área operacional en definitiva esta también ligada a la capacitación del personal involucrado, y en la actualidad aún es una de las deficiencias que impedirían una implementación oportuna.

3.4 EN EL ASPECTO ECONOMICO

Hay que tomar en cuenta que para la implementación de un Sistema de Gestión de Seguridad de la Información, se requiere invertir tanto en capital humano, como en tecnología. Esto traducido a la aplicabilidad de esta propuesta Modelo de Sistema de Gestión de Seguridad de la información en el ISTAC, nuestro análisis nos permitió deducir que financieramente se requiere de lo siguiente:

PRODUCTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Asesoría especializada	80 horas	$ 80,00	6400,00
Licencias informáticas	4	$ 200,00	800,00

No se hace constar el equipamiento de hardware, ya que hace dos meses fueron adquiridos seis servidores Samsung.

JUSTIFICATIVO

Ya que en resumen nuestro modelo de SGSI, basado en la normativa ISO 27001 y 27002, cubre:

a) Política de Seguridad.
b) Aspectos organizativos para la seguridad.
c) Clasificación de Activos.
d) Control.
e) Seguridad ligada al personal.
f) Seguridad física y del entorno
g) Gestión de Comunicaciones y Operaciones
h) Control de Accesos
i) Desarrollo y mantenimiento de sistemas
j) Gestión de continuidad del negocio
k) Conformidad con la legislación y reglamentación existente

De estos once dominios se derivan 39 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 133 controles (practicas, procedimientos o mecanismos que reducen el nivel de riesgo).

En esta implementación ensayo del modelo debería participar un equipo mínimo de 4 personas que tendrían un costo mínimo de $20,00 dólares la hora por persona, que tendrían que realizar lo siguiente:

ACTIVIDAD	OBJETIVO
Pre-auditoria (revisión)	Analizar y revisar in situ las líneas generales del Modelo SGSI,para adaptarle al Instituto (Alcance)
Estudio documental	Valorar la adaptación del Modelo de SGSI, contra la norma y aportar el feedback al Instituto
Fase inicial	Revisar y confirmar la posible implantación del Modelo SGSI contra la norma ISO 27000
Seguimiento	Cerciorarse el cumplimiento del Modelo SGSI.

Este Instituto cuenta con recursos económicos provenientes de su POA Plan Operativo Anual que es revisado cuatrimestralmente por disposición gubernamental. Consultadas las principales partidas presupuestarias, en coordinación con el área de informática, nos permitieron observar que sería factible, utilizar dos de ellas:

- La partida No 5306, cuyo rubro es: consultoría, asesoría e investigación especializada.
- La partida No 5307, cuyo rubro es: arrendamiento licencias uso paquetes informáticos.

Cabe recalcar que estos costos fueron establecidos en base a un **análisis beneficio costo**, y en base a la decisión con el equipo de participantes sobre la base de: **hago o compro**, debido a la actual situación económica por la que atraviesa este Centro de Instrucción Aeronáutica, que básicamente es limitada, ya que si bien como centro educativo genera recursos económicos propios que podrían solventar su autogestión, sin embargo se encuentra limitada ya que todos estos recursos son enviados a la Dirección General de Aviación Civil por disposiciones financieras legales.

Además que en procura de hacer una gestión integral es mejor subcontratar, por tratarse de servicios especializados, lo que evitaría incrementar nomina o incurrir en gastos de capacitación, entrenamiento, etc., cumpliendo también con la actual

Ley de Presupuestos del sector Publico, que permite reorientar los gastos dentro de la misma línea de lo que ya se encuentra planificado, pudiendo por lo tanto tener una inmediata aplicación a los gastos actuales.

CAPITULO 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Los riesgos son implícitos a estos Institutos Tecnológicos de Educación Superior Aeronáutica y por lo general a todo tipo de organizaciones, su adecuado tratamiento y Gestión implica un cambio de actitud de toda la organización.

Los Institutos Superiores Tecnológicos de Educación Aeronáutica, no realizan una Gestión formal de la Seguridad de la Información, y no disponen de un Sistema de Gestión de Seguridad de la Información, debido más a la falta de interés y básicamente por un desconocimiento de su utilidad.

La Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información es de uso genérico y permite que los procesos de los Institutos de Educación Superior Aeronáutica, se vuelvan mas formales y sobre todo documentados, optimizando por tanto el funcionamiento de la Seguridad de la Información.

El uso adecuadamente combinado de la Norma ISO 27002:2005 (Mejores Practicas), que no permite certificaciones, con la Norma ISO 27001:2005 , que si es certificable, en la implementación de un Sistema de Gestión de Seguridad de la Información SGSI constituye el camino adecuado hacia el éxito en los Sistemas Educativos.

El punto concluyente de un Sistema de Gestión de Seguridad de la Información es facilitar a un Instituto de Educación Superior Aeronáutica determinar el establecimiento de Políticas de Seguridad de la Información, para todos los niveles de su estructura organizacional asegurando conformidad con su Misión y objetivos estratégicos.

En este como en todos los proyectos de implementación, un aspecto importante es que deben ser socializados, antes durante y después; si se quiere realmente resultados de calidad

4.2 RECOMENDACIONES

Es importante que en todo momento y principalmente en la planificación de la Gestión de la Seguridad de la Información se considere el tratamiento de los Riesgos, como una área más de conocimiento, es decir una Gerencia de Riesgos, no solo para evitarlos o minimizar su efecto, sino que se constituya un proceso iterativo de Saber que hacer, y como hacerlo con la oportunidad del caso, característica única de una Gestión de calidad.

Es preocupación de las Direcciones de estos Institutos de Educación Superior el formalizar una adecuada inducción a la utilización de un Sistema de Gestión de Seguridad de la Información o por lo menos arrancar con socializar la idea del riesgo y el efecto de no asegurar la información en función del beneficio-costo.

Se sugiere al ISTAC Instituto Superior Tecnológico de Aviación Civil, usar la presente Propuesta Modelo, de modo referencial como instrumento de su Planificación y Gestión Estratégica.

Para el corto plazo, sugerir a los directivos de la Dirección de Aviación Civil para que a través del establecimiento de acuerdos con Universidades que utilizan Tecnología de punta, mejoren los procesos de seguridad del ISTAC, de manera aún más segura utilizando la infraestructura de seguridad que ellas poseen. Logrando también mejores niveles de profesionalización y reconocimiento. Así como se asocien, y soliciten el apoyo de otros organismos internacionales interesados en difundir la educación aeronáutica en forma virtual.

Intencionalmente
en Blanco

BIBLIOGRAFIA

1. SLADE, Robert M. Security Frameworks: Theory and Case Studies. Editorial IRM Press. United States. 2006.

2. INFORMATION SECURITY FORUM ISF , http// www.ifsecuritystandar.com/pdf/standar.pdf David;

3. Risk Management Guide for Information Technology Systems 800-30, http://csrc.nist.gov

4. Generally Accepted Principles and Practices for Securing Information Technology Systems 800-14, http://csrc.nist.gov

5. An Introduction to Computer Security: The NIST Handbook 800-12, http://csrc.nist.gov

6. Engineering Principles for Information Technology Security 800-27, http://cscr.nist.gov

7. Recommended Security Controls for Federal Info Systems 800-53, http://cscr.nist.gov

8. OACI ORGANIZACION DE AVIACION CIVIL INTERNACIONAL, Boletín de Resultados de la Reunión de Directores de Centros de Instrucción de Aviación Civil, Quito-Ecuador 24 octubre 2001

9. ARGENTERO, Cristian. La Seguridad Informática no es producto sino un proceso. Buenos Aires.2006

10. KAPLAN, Robert. The Balanced Scorecard. Ed. Instituto de Empresa. Madrid. 2007.

11. BEATH, Carl; ROSS, James. Beyond the Business Case: New approaches to IT Investment. MIT Sloan Management Review. Winter 2002.

12. Plan Digital de Chile para el 2007-2012, www.estrategiadigital.gob.cl. Diciembre 2007.

13. NORMA ISO 27001, http//:ISO27001.security.com/html/white_papers.html. Mayo 2008

ANEXOS

ANEXO 1 ENCUESTAS……CD

ANEXO 2 NORMA ISO 27001:2005……CD

ANEXO 3 NORMA ISO 27002:2005……CD