U M S N H

Facultad De Contaduría y Ciencias Administrativas
Tesis:

Seguridad De la Información En Las Organizaciones

(Caso sistema kardex de posgrado de la FCCA)

Para obtener el título de:

Lic. Informática Administrativa

Ma. Del Rocío Lemus Zamora

Asesor:

DR. M. Gerardo Alfaro Calderón

ENERO DEL 2010

ÍNDICE

Introducción

La información: Bajo el punto de vista de la ingeniería: Estudio de las características y estadísticas del lenguaje que nos permite su análisis desde un enfoque matemático, científico y técnico.
Bajo el punto de vista de la empresa: Conjunto de datos propios que gestionar y mensajes que se intercambian personas y/o maquinas dentro de una organización.

Información externa entre los estudios para clasificar la información del entorno de la empresa destaca, también, la clasificación de Laudon y Laudon que sirve, además, para estructurar la captura y absorción de información.
La Información interna: En todo proceso de toma de decisiones se necesita información externa. Sin embargo para que dicha información pueda ser dirigida por los gestores requiere que sea tratada internamente. Además, es necesario que la información pueda fluir por los canales de la empresa para que obtenga el máximo provecho por parte de la organización. Nos referimos, también, a la información formal y a la informal.

La importancia de la Información para las organizaciones, puede ser vista desde los siguientes puntos de vista básicos: Que cumplan con su función primordial, es decir, la de aumentar el conocimiento del usuario o en reducir sus incertidumbres. Valor Administrativo, Valor Operacional, Valor Histórico
Generador de nuevos factores de competitividad Integrador de las unidades de la organización.
Tipos de información: Operacional: Es aquella que resulta del propio funcionamiento diario de la organización.
De Conocimiento: Las empresas generan conocimientos como resultado de la asimilación y análisis de información interna y externa y de la explotación de las capacidades creativas de sus miembros cuando se diseñan nuevos productos, se mejoran o incorporan nuevos procesos productivos y administrativos.
Los Directivos y la Información: Todos los miembros de la Organización, en especial los cargos directivos utilizan la información en una mayor o menor medida, dependiendo de la posición jerárquica y el tipo de toma de decisión.

Nivel Estratégico. Nivel Táctico, Nivel Técnico u Operativo.

Las organizaciones: Una organización es cualquier institución compuesta de recursos, cuya combinación, permite alcanzar una serie de objetivos. El ser humano vive y se relaciona dentro de organizaciones, lo que ha dado lugar a que nuestra sociedad haya sido denominada "burocrática" u "organizacional".

Las organizaciones pueden ser definidas por sus estructuras, formadas por múltiples canales y normas. La organización es un complejo de canales a través de los cuales los productos, servicios, recursos y flujos de información transitan de un punto a otro dentro de la organización, y también entre la organización y su entorno.

La información es un recurso estratégico más de la empresa. El personal de la empresa, los medios materiales y económicos son considerados recursos de la misma porque generan unos rendimientos, es decir, son productivos. Pero la información también produce rendimientos ya que tiene la misión de informar, revelar alternativas, reduce incertidumbres y desvela soluciones entre otras cosas.

La Información como Producto: Para que la información sea gestionada como un producto ha de seguir varios estadios.

Gestión de recursos de Información (GRI): La mayoría de las organizaciones posee gran cantidad de datos pero escasa información de gestión. La gestión consiste en la transformación de información en acciones mediante criterios. Ante una gran acumulación de datos y poca información de gestión se suele caer en el error de pedir más y más información. .

La forma mas inteligente para lograr la seguridad de la información es analizando cada uno de los elementos que nos permiten conocer como es en realidad la situación que se presenta en las organizaciones, y que interviene en ello, saber detalladamente los vínculos entre estos factores que nos llevan a tener un éxito o fracaso en nuestros objetivos, el desempeño que se está dando sobre una seguridad que no significa que no existan errores, si no que sabemos que los hay y cual sería nuestra respuesta ante esta situación.

En la actualidad las organizaciones se están dando cuenta de que la información es lo de ahora, es vital para el buen desarrollo de nuestros proyectos se podría decir que todos hemos utilizados la información para logra

algo, pero que tan indispensable será que esa información llegue a cambiar nuestros planes por una ignorancia en la administración de ella.

La importancia de la información, sus factores, vulnerabilidades que hoy en muchas empresas o organizaciones aun no se toman en cuenta a pesar del impacto que se esta dando, los beneficios que consigo lleva al saber utilizarla de manera adecuada y con la seguridad que requiere.

Protocolo

Definición del problema

El poco conocimiento o nulo sobre la administración de la información así como la necesidad de conocer herramientas para su mejor aprovechamiento dentro de una organización, el valor que se otorga a la información, saber que tan importante llega a ser este nuevo recurso como una ventaja competitiva en cualquier negocio.

Justificación del problema

Las organizaciones necesitan de seguridad en su información para poder penetrar el mercado, en la actualidad hay empresas que por la falta de una buena administración de su información dan marcha a que otras vivan de ellas, de ahí a que se conozca la importancia y el manejo para su mayor utilidad, comprendiendo lo anterior se puede lograr la fase en que la información debe resguardarse ante cualquier percance por insignificante que este pueda llegar a ser, la necesidad de tener siempre a la mano dicha información y que esta pueda llegar a ser lo suficientemente integra para poder tomarla a favor de un bien en la organización.

Preguntas de investigación

1. ¿Cuáles son algunas metodologías para el manejo de la información?
2. ¿Qué herramientas necesito para la administración de la información?
3. ¿Cuáles puntos son claves para la utilización de la información?
4. ¿Qué aspectos se toman en cuenta para la protección de la información?
5. ¿A qué información se le otorga protección?
6. ¿Métodos para lograr la seguridad de la información?
7. ¿Qué cambios se lograr con la seguridad de la información en las organizaciones?

Objetivo general

Proponer elementos de seguridad de información al sistema de Kardex del posgrado de la facultad de contaduría y ciencias administrativas.

Objetivo Especifico

Determinar el nivel de Seguridad del Sistema kardex del posgrado de la FCCA.

Marco Teórico

Capítulo I La Información

Bajo el punto de vista de la ingeniería: Estudio de las características y estadísticas del lenguaje que nos permite su análisis desde un enfoque matemático, científico y técnico. [1]
Bajo el punto de vista de la empresa: Conjunto de datos propios que gestionar y mensajes que se intercambian personas y/o maquinas dentro de una organización. [1]

En una organización la información es el conjunto de datos, ficheros, mensajes intercambiados, historial de clientes y proveedores, así como la historia de los productos sin dejar de mencionar que cualquier dato dentro de la empresa representa la información con la que la empresa cuenta por insignifícate que parezca o tan innecesario que se vea.
El éxito de la empresa depende de la calidad de la información que genera y gestiona. La información es de calidad si posee: Confidencialidad, Integridad, Disponibilidad.

Confiabilidad. Será autorizada solo por aquellos usuarios autorizados
Integridad. La información solo será modificada por los usuarios autorizados
Disponibilidad. El usuario debe de disponer de la información en el momento y lugar donde la necesite.

Sea eliminada, sea alterada, sea utilizada en contra de la empresa, sea conocida por personal no autorizado, sea utilizada con fines de lucro.

Desde el punto de vista de la organización la información se verá afectada por Uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, bien por factores externos o internos. El factor humano interno.

1.1 Información externa (modelo de laudon y laudon).

Entre los estudios para clasificar la información del entorno de la empresa destaca, también, la clasificación de Laudon y Laudon [2] que sirve, además, para estructurar la captura y absorción de información (volveremos sobre estos conceptos al identificar en un apartado posterior el contexto en el que se mueve una empresa).

Así, identifican dos entornos, inmediato y remoto:

El entorno inmediato, lo conforman los activos que una empresa trata a diario, como clientes, distribuidores, competidores, proveedores, financiadores y reguladores.

El entorno remoto, está formado por aquellos elementos que una empresa debe tener en cuenta para controlar el entorno en el que se encuadra, y que está formado por la información sobre la situación política, la sociedad, los cambios tecnológicos o la evolución económica.

1.1.1La Información interna.

En todo proceso de toma de decisiones se necesita información externa. Sin embargo para que dicha información pueda ser dirigida por los gestores requiere que sea tratada internamente. Además, es necesario que la información pueda fluir por los canales de la empresa para que obtenga el máximo provecho por parte de la organización. Nos referimos, también, a la información formal y a la informal.

Diferencia entre dos tipos de información interna: los conocimientos y la información operacional. La información operacional es la generada por la organización debido al funcionamiento rutinario de la empresa; mientras el conocimiento es el resultado de la fusión de la información interna y externa, que genera beneficios para las empresas [3].

1.2 La importancia de la información

Una empresa es más competitiva cuanto más se destaca en la explotación de la Información del entorno.

La importancia de la Información para las organizaciones, puede ser vista desde los siguientes puntos de vista básicos:

1. Que cumplan con su función primordial, es decir, la de aumentar el conocimiento del usuario o en reducir sus incertidumbres. En este sentido el valor de la Información está relacionado en la forma en que ayude a los individuos dentro de la organización para que tomen las decisiones que lo conduzcan a lograr los objetivos y metas propuestas.

Sin embargo se podrá clasificar el valor de la Información de acuerdo a:

Valor Administrativo: Cuando la información permite a la Gerencia tomar decisiones efectivas.

Valor Operacional: Cuando la información apoya o documenta las actividades de rutina o repetitivas de la Organización. Ejem. Los manuales.

Valor Documental: Cuando sirve de prueba o evidencia sobre los hechos ocurridos en la Empresa. Ejem: La información suministrada por la factura de compra y venta.

Valor Histórico: Cuando la información nos documenta sobre los hechos pasados o nos provee de elementos para estimar comportamientos futuros. Ejem.: El comportamiento de las ventas del año 1997 nos permite realizar las proyecciones para el año 1998.

2. Generador de nuevos factores de competitividad: La competitividad no depende solamente de la capacidad que tenga la Empresa de ofrecer un producto a mejor precio que sus competidor, sino también de lo que realmente requiere el Público consumidor o que es lo que el cliente valora realmente (calidad, servicio, atención posventa). Este proceso de identificación de valores, requiere de un afinado mecanismo de obtención de información procedente del entorno de la Empresa.

Pero no sólo se trata de disponer de información sobre el entorno, sino también de obtenerla antes que los competidores, lo que obliga a la sistematización de la captura y el procesamiento de los datos para su posterior análisis.

3. Integrador de las unidades de la organización: La información obtenida por una unidad puede resultar de gran utilidad para otras unidades, incluso para aquellas que aparentemente parecen menos relacionadas.

4. En la medida que mejora de los procesos productivos y administrativos: Que se logra con toda aquella información que incrementa la tecnología del conocimiento del recurso humano de la organización. Dicha información la obtenemos por medio de los
Centros Educativos, Cursos y Revistas especializadas, Desarrollo Personal, entre otros Tipos Información del Entorno Organizacional (Ambiental)

Concepto: Entrada de información en la empresa procedente del entorno.
Captar información sobre el mercado permite responder a sus necesidades.
Captar información tecnológica asegura explotar las posibilidades tecnológicas existentes en el entorno. El desarrollo de los activos invisibles como la capacidad de responder a las necesidades del mercado o la adquisición de habilidades tecnológicas, depende de la habilidad con que se maneje el flujo de información ambiental entrante en la Empresa.
Las empresas tradicionalmente, por diversas razones han confiado mas en los procedimientos informales, pero varios factores las están obligando a cambiar de actitud:

- La globalización de la economía: Cada vez existen menos barreras fronterizas y todas tienen oportunidad de penetrar en el mercado mundial, las empresas ya no pueden seguir confiando en sus fuentes tradicionales, por lo general son de nivel nacional, requieren información de los mercados internacionales para estar al día de nuevos proveedores y competidores, los requerimientos y necesidades de los clientes, condiciones impositivas y calidad de los productos de sus competidores.

- La velocidad del proceso tecnológico: Las empresas deben adecuarse a las nuevas tecnologías, que les permitan mantenerse dentro de un mercado cada vez más competitivo. Las empresas deben evitar rezagarse con respecto a sus competidores. Es decir, comparar una compañía con aquellos líderes en mercado ya sea en calidad de sus productos o en la aplicación de innovadores procesos administrativos y tecnológicos.
[16]

1.3 Tipos de información

Operacional: Es aquella que resulta del propio funcionamiento diario de la organización: Como ejemplo de ésta tenemos: Listas de productos, clientes y proveedores, ventas y gastos (presupuesto), entre otros. Esta información es fundamentalmente formal y es almacenada en diferentes dispositivos, ya sean manuales o electrónicos.

De Conocimiento: Las empresas generan conocimientos como resultado de la asimilación y análisis de información interna y externa y de la explotación de las capacidades creativas de sus miembros cuando se diseñan nuevos productos, se mejoran o incorporan nuevos procesos productivos y administrativos.

Los Directivos y la Información: Todos los miembros de la Organización, en especial los cargos directivos utilizan la información en una mayor o menor medida, dependiendo de la posición jerárquica y el tipo de toma de decisión. Consideramos los tres niveles básicos que conforman la Pirámide Organizacional.

1. Nivel Estratégico: Está en manos de los directivos de alto nivel (accionistas, gerentes generales y en algunos casos gerentes medios). En este nivel se toman decisiones sobre los objetivos a largo plazo de la empresa, los recursos necesarios para conseguirlos y sobre los procedimientos generales. Por ejemplo, decisiones referidas a la expansión de la planta, la diversificación de

la producción, aumentos de capital, incorporación de nuevos socios, entre otros. Estas decisiones estratégicas, están caracterizadas por un alto grado de incertidumbre, y requieren de una gran cantidad de información, tanto interna, como externa que nutran la capacidad de los tomadores de decisiones.

2. Nivel Táctico: Está en manos de los directivos del nivel medio (gerentes sectoriales o jefes de departamento), tienen como función primordial dirigir y supervisar las funciones que se realizan dentro de la organización para que de esta forma se pueda cumplir con los objetivos y metas trazadas. Los directivos de este nivel requieren de una mezcla equilibrada de información interna y externa. Es decir, se utiliza información proveniente de las mismas operaciones de la Empresa, así como información proveniente de los clientes, proveedores, y estudio de mercado, que le sirven para controlar los procesos y medir el grado de cumplimiento de los objetivos trazados por el nivel estratégico.

3. Nivel Técnico u Operativo: En manos de los directivos de primer nivel conformado por los jefes de secciones y en algunos casos jefes de departamentos. Tienen como objetivo fundamental, verificar las tareas diarias de las distintas secciones o departamentos. En este nivel se requiere información sobre el desarrollo diario de las operaciones de la Empresa, por ejemplo información generada por los distintos departamentos y secciones en forma de monitoreo de trabajo e informes de funcionamiento. Este nivel requiere de información externa, tal como la necesaria para el manejo de mantenimiento de los equipos y maquinarias, repuestos y suministros.

1.4 Las organizaciones

Una organización es cualquier institución compuesta de recursos, cuya combinación, permite alcanzar una serie de objetivos. El ser humano vive y se relaciona dentro de organizaciones, lo que ha dado lugar a que nuestra sociedad haya sido denominada "burocrática" u "organizacional". [4]

Las organizaciones pueden ser definidas por sus estructuras, formadas por múltiples canales y normas. La organización es un complejo de canales a través de los cuales los productos, servicios, recursos y flujos de información

transitan de un punto a otro dentro de la organización, y también entre la organización y su entorno [5].

1.4.1 La Información en las organizaciones

Itami, profesor japonés estudioso sobre la importancia de la información en la empresa moderna, considera que la información en la empresa tiene tres características: puede ser utilizada simultáneamente, no se gasta con el uso, y sus trozos pueden ser combinados para generar más información [6].Para Itami, los recursos que realmente cuentan son los que denomina invisibles, como por ejemplo, la capacidad para aprender, de asimilar y crear tecnología. Estos activos se nutren gracias a los flujos de información básicos: el de la información que entra en la empresa procedente de su entorno (la información ambiental), la información que fluye por la empresa (información interna), y la información que la empresa proyecta hacia el exterior (información corporativa).

La información externa que le llega al empleado y que le sirve para realizar su trabajo debe de ser de calidad. Por ello, la calidad de esta información tiene que asegurarse en el centro donde es recibida y procesada, en el centro de información de la empresa, que debe ser también el centro de operaciones del sistema de información y de aseguramiento de la calidad informativa [7]. No hay que olvidar que un trabajo elaborado con calidad genera una información de calidad.

La misión de un centro de información empresarial es la de ofrecer a sus usuarios una información de calidad que les permita tomar decisiones, por lo que hay que implantar un programa de gestión de calidad, incluido en el sistema de gestión de calidad total de la empresa. En este programa, todos los miembros del centro tienen que cumplir ciertas tareas, es decir, se especializa a cada empleado en una tarea concreta.

En el momento en que la empresa decide abrir las puertas a la información, ésta debe ser correcta y actual, debe cubrir las necesidades del receptor, tiene que estar disponible cuando el receptor lo precise, y no será para todos, ya que existe la privacidad.

Lo que caracteriza a la información en una empresa, es su capacidad de intercambio [8]. La información es un producto perecedero, y almacenarla únicamente para archivarla pierde interés. Lo verdaderamente importante es encontrar la información más reciente rápidamente, acceder a la fuente y crear la información.

No hay duda que la información representa el activo más crítico para que una organización logre el éxito de los objetivos de negocio o estratégicos, es decir, aquellos que son fundamentales y representan la razón de ser de la empresa.

Las características necesarias para la existencia de todo sistema de información [9]:

Disponibilidad de información cuando es necesario y por los medios adecuados. Suministro de información de manera selectiva.

Variedad en la forma de presentación de la información.

Grado de inteligencia incorporado al sistema.

Tiempo de respuesta del sistema.

Exactitud.

Generalidad, como las funciones para atender a las diferentes necesidades.

Flexibilidad, capacidad de adaptación.

Fiabilidad, para que el sistema opere correctamente.

Seguridad, protección contra pérdidas.

Reserva, nivel de repetición del sistema para evitar pérdidas.

Amigabilidad, para el usuario.

1.5 La Información como Recurso

Diebold (1979) introdujo el concepto de que la información debía ser manejada como un recurso fundamental en la empresa. Más tarde, Synott y Gruber inauguraron una línea de pensamiento basada en la convicción de que la información merecía recibir una mayor consideración por las empresas.

La información es un recurso estratégico más de la empresa. El personal de la empresa, los medios materiales y económicos son considerados recursos de la misma porque generan unos rendimientos, es decir, son productivos. Pero la información también produce rendimientos ya que tiene la misión de informar, revelar alternativas, reduce incertidumbres y desvela soluciones entre otras cosas [10]. Es un rendimiento más importante o relevante de lo que parece ya que ayuda a la toma de decisiones. La información se convierte en un recurso de toda la empresa no sólo de la dirección que es la que en principio posee el poder dentro de la organización. Además, resulta fundamental ya que los activos intelectuales a diferencia de los activos físicos, aumentan su valor con el uso [11].Como tal, tiene un valor de mercado (es bajo y está relacionado con su obtención, elaboración, mantenimiento y distribución), y valor de uso, que es mucho mayor y depende de para qué se va a usar. El valor de la información se deriva del aumento que debe originar en el rendimiento de la empresa [12].

Hay dos características del recurso información que le distinguen de otros recursos de la empresa: su intangibilidad, por lo que se hace muy difícil de manejar y gestionar (muchos empresarios no le conceden la importancia que debieran por lo difícil que es demostrar la eficacia de su rendimiento); y su incombustibilidad, ya que la información no se gasta sino que se puede modificar y actualizar con un bajo coste adicional.

1.6 La Información como Producto

Wang, Lee, Pipino y Strong (1999) identifican la información como producto. Las conclusiones de su estudio alertan de que la mayoría de las empresas gestionan la información erróneamente ya que se centran en los sistemas, en el ciclo de vida del hardware y el software que generan la información, cuando deberían hacerlo por sus contenidos.

Para que la información sea gestionada como un producto ha de seguir varios estadios: conocer las necesidades de información de los empleados, gestionar la información como un producto de un proceso de producción que tiene un ciclo de vida, y por último, designar a un responsable IPM (Information Product Manager), que gestione los procesos de información y el producto resultante. El IPM es muy diferente del CIO ya que el primero se encarga de la producción y entrega de la información en un sistema que cuente con la participación de los usuarios, suministradores y productores. La tarea del CIO es la de control de las entradas de datos en las bases de datos.

El enfoque de información como producto tiene la finalidad de proporcionar al usuario una información de calidad. Los usuarios califican una información de calidad cuando reúne las siguientes características: calidad intrínseca (precisión, objetividad, credibilidad, reputación), calidad de accesibilidad a la información (accesibilidad, facilidad de tratamiento, seguridad), calidad contextual de la información (relevancia, valor añadido, puntualidad, carácter completo, cantidad de información), y calidad representativa de la información (interpretar, facilidad de comprensión, representación concisa y coherente)[13].

La utilización de las tecnologías de la información proporciona esa información de calidad. Pero hay que advertir que muchas web de empresa están abandonadas por sus creadores, es decir, no tratan las páginas web como un producto de información.

En muchas ocasiones los departamentos de tecnologías de la información se preocupan demasiado por la calidad del sistema de entrega y sus componentes en vez de optimizar la calidad del producto de información. Para ello, se necesita un conocimiento profundo de las necesidades de información y los criterios de calidad del usuario.

Centrarse únicamente en el sistema informático supone que a la información inicial no se le presta atención en los cambios de vida del producto de información.

Por último, adoptar un enfoque de información como producto mejora la comunicación interna, las actividades son más eficientes y repercute en la mejora de la rentabilidad, competitividad y la posición en el mercado. Aceptar la información como un proceso de producto implica que este proceso ha de estar bien definido y controlado y una buena gestión en el tiempo de producción y entrega de la información.

1.7 Gestión de recursos de Información (GRI)

La mayoría de las organizaciones posee gran cantidad de datos pero escasa información de gestión. La gestión consiste en la transformación de información en acciones mediante criterios. Ante una gran acumulación de datos y poca información de gestión se suele caer en el error de pedir más y más información. Nació un nuevo concepto de gestión empresarial que fue bautizado como Gestión de Recursos de Información (GRI).

Gestión de los sistemas de información. Aunque exista una complejidad técnica no hay que descuidarlo por la alta dirección de la empresa. Es decir, debe haber un diálogo fluido entre la dirección y el departamento técnico.

Objetivo de la función de gestión de información. Esta función es la de proveer servicios de la mejor calidad para lograr los objetivos de la organización.

Integración en el equipo de dirección. La persona responsable de la gestión de la información debe formar parte del equipo de la alta dirección de la empresa.

Independencia de la función de información. La persona que ejerza la gestión de información en el organigrama debe garantizar su independencia, es decir, debe estar en condiciones de servir a toda la organización sin recibir presiones.

La comunicación como una clave de éxito. Debe existir comunicación entre los diseñadores de los sistemas de información y los usuarios para conocer sus necesidades.

La cultura de la empresa. La gestión de la información se debe corresponder con la cultura de la organización, de lo contrario el objetivo de la integración de los sistemas con la organización del usuario es imposible.

La GRI es hoy una disciplina en la que participan profesionales procedentes de tres áreas aparentemente lejanas: administración de empresas, informática y ciencias de la información. Es el proceso de construir y gestionar la infraestructura tecnológica de la empresa, y trata de la conducción de la información mediante hardware (ordenadores, comunicaciones, redes, ofimática). Su finalidad última es ofrecer mecanismos que permitan a la organización adquirir, producir y transmitir al menor coste posible, datos e información con una calidad, exactitud y actualidad suficientes para servir a los objetivos de la organización.

Los fundamentos de la GRI son básicamente tres: la convicción de que es el contenido de la información y no su forma o soporte lo que realmente importa. Después, la afirmación de que el gasto de alternación de información y tecnologías de la información no debe considerarse dentro del capítulo de gastos generales de funcionamiento, sino como la adquisición de un recurso que puede ser usado para la reducción de costes de operación en otras áreas de la empresa. Y por último, la convicción de que es preciso coordinar los recursos de información y tecnologías de la información, actualmente muy dispersos por las organizaciones.

En cuanto a sus componentes la GRI debe tratar con tres funciones distintas: las tecnologías de la información, que hoy en día constituyen la columna vertebral de la gestión de la información; los sistemas de información, entendidos como el resultado de transformar la tecnología en algo de valor para el usuario; y la gestión de la información y de los conocimientos de la organización.

No cabe duda que la información representa el activo más crítico para que una organización logre el éxito de los objetivos de negocio o estratégicos, es decir, aquellos que son fundamentales y representan la razón de ser de la empresa. Los objetivos de negocio pasan por conseguir que la información, cualquiera que sea su soporte y su ciclo de vida dentro de la organización, sea analizada bajo distintos requerimientos: de calidad, financieros, de seguridad, legales, u

otros que puntualmente puedan ser necesarios. Dichos requisitos guiarán a los recursos y procesos empleados en los sistemas de información para conseguir los objetivos estratégicos fijados.

De hecho, nadie pone en duda que la “información es poder” por lo que muchas organizaciones disponen los recursos necesarios para su obtención y control, ya que ésta y la tecnología de información ayudan al desarrollo competitivo de las mismas, diferenciándolas de la competencia, creando nuevos productos y servicios, nuevas barreras de entrada, etc.

1.8 La Información como Recurso de las Organizaciones

Desde hace ya algunos años las organizaciones han reconocido la importancia de administrar los principales recursos como la mano de obra y las materias primas.

La información se ha colocado en un buen lugar como uno de los principales recursos que poseen las empresas actualmente. Los entes que se encargan de las tomas de decisiones han comenzado a comprender que la información no es sólo un subproducto de la conducción empresarial, sino que a la vez alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de estos.

Si deseamos maximizar la utilidad que posee nuestra información, el negocio la debe manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes. Los administradores deben comprender de manera general que hay costos asociados con la producción, distribución, seguridad, almacenamiento y recuperación de toda la información que es manejada en la organización. Aunque la información se encuentra a nuestro alrededor,

debemos saber que ésta no es gratis, y su uso es estrictamente estratégico para posicionar de forma ventajosa la empresa dentro de un negocio.

La fácil disponibilidad que poseen las computadoras y las tecnologías de información en general, han creado una revolución informática en la sociedad y de forma particular en los negocios. El manejo de información generada por computadora difiere en forma significativa del manejo de datos producidos manualmente.

1.9 Sistemas de Información

Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware). Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado".

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un sistema de información realiza cuatro actividades básicas:
Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.
Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardad en la sesión o proceso anterior.
Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador

de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, cintas magnéticas, diskettes, la voz, etc.

1.10 Tipos y usos de los Sistemas de Información

Durante los próximos años, los sistemas de información cumplirán los siguientes objetivos:

Automatizar los procesos operativos:

Proporcionar información de apoyo a la toma de decisiones.

Lograr ventajas competitivas a través de su implantación y uso.

Con frecuencia, los sistemas de información que logran la automatización de procesos operativos dentro de una organización son llamados Sistemas Transaccionales, ya que su función consiste en procesar transacciones tales como pagos, cobros, pólizas, planillas, entradas, salidas. Por otra parte, los sistemas de información que apoyen los procesos de toma de decisiones son los sistemas de apoyo a la toma de decisiones (DSS, por sus siglas en inglés Decisión Supporting System). El tercer tipo de sistemas, de acuerdo con su uso u objetivos que cumplen, es de los Sistemas Estratégicos, los cuales se desarrollan en las organizaciones con el fin de lograr las ventajas competitivas, a través del uso de la Tecnología de Información (TI).

1.11 Importancia de los Sistemas de Información

Muchas veces las organizaciones se han entrado en la etapa de cambio hacía la era de la información sin saber que es un riesgo muy grande de fracaso debido a las amenazas del mercado y su incapacidad de competir, por ejemplo, las TI que se basan en Internet se están convirtiendo rápidamente en un ingrediente necesario par el éxito empresarial en el entorno global y dinámico de hoy.

Por lo tanto, la administración apropiada de los sistemas de información es un desafío importante para los gerentes. Así la función de los SI representa:
Un área funcional principal dentro de la empresa, que es tan importante para el éxito empresarial como las funciones de contabilidad, finanzas, administración de operaciones, marketing, y administración de recursos humanos.
Una colaboración importante para la eficiencia operacional, la productividad y la mora del empleado, y el servicio y satisfacción del cliente.
Una fuente importante de información y respaldo importante para la toma de de decisiones efectivas por parte de los gerentes. Un ingrediente importante para el desarrollo de productos y servicios competitivos que den a las organizaciones una ventaja estratégica en el mercado global.
Una oportunidad profesional esencial, dinámica y retadora para millones de hombres y mujeres.

Frecuentemente se ha utilizado el término informatización como sinónimo de sistemas de información. Y aunque la mayoría de los autores están de acuerdo en asumir que un sistema de información requiere un adecuado proceso de informatización, lo que también está claro es que no en todos los casos la construcción de un sistema de información lleva aparejado el uso de tecnologías de la información [14].

1.12 Una sociedad de Información Global

Estamos viviendo en una sociedad de información global emergente, con una economía global que depende cada vez más de la creación, la administración y la distribución de la información a través de redes globales como Internet. Muchas empresas están en proceso de globalización; es decir, se están convirtiendo en empresas globales interconectadas en red. Por ejemplo, las empresas se están expandiendo a mercados globales para sus productos y servicios, utilizando instalaciones de producciones globales para fabricar o ensamblar productos, reuniendo dinero en mercados de capitales globales, formando alianzas con socios globales y luchando con competidores globales pro clientes de todo el mundo. El manejo y la realización de estos cambios estratégicos serían imposibles sin Internet, Intranets y otras redes globales de computación y de telecomunicaciones que constituyen un sistema nervioso central de las empresas globales de hoy.

1.13 Un enfoque global de la Información

Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se le compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas. Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos:

Concienciar a los usuarios acerca de los problemas de seguridad

Seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.

Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.

Seguridad física, o la seguridad de infraestructuras materiales: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

1.14 La seguridad

La seguridad física: puede asociase a la protección del sistema o la información ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de acceso apersonas etc.
La seguridad lógica: protección de la información en su propio medio, mediante ocultamiento de la misma usando técnicas de criptografía.
La gestión de la seguridad esta en medio de las dos.

1.14.1 La seguridad de la Información

Aplicando un proceso sistemático, documentado y conocido por toda la organización que permita garantizar, no que la empresa es completamente segura, sino que conoce los riesgos a los que se enfrenta, los ha evaluado, los sabe gestionar y los ha minimizado de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el sistema de información.
En la actualidad, cada vez menos las inversiones en seguridad que realizan las empresas se están destinando exclusivamente a la compra de productos, sino que comienzan a dotar parte de su presupuesto para destinarlo a la gestión de la seguridad de la información. El concepto de seguridad ha variado, recalcándose un nuevo concepto: “seguridad gestionada”, que ha desbancado al de “seguridad informática”. Las medidas que comienzan a tomar las empresas giran entorno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes técnica, legal y organizativa, es decir un planteamiento coherente de directrices, procedimientos y criterios que permiten desde la dirección de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de Información, la organización afín y sus

infraestructuras. Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que “la seguridad absoluta no existe”.

Tomando como referencia esta máxima, una entidad puede adoptar alguna de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información. El presente artículo se va a centrar en una de ellas, concretamente en la norma UNE 71502 / ISO 17799.

La norma UNE/ISO/IEC 17999 es un código de buenas prácticas para gestionar la seguridad de la información de una organización, de tal forma que le permita en todo momento la confidencialidad, integridad y disponibilidad de la información que maneja. La creación de esta norma responde a la necesidad de proporcionar una base común, a las organizaciones, de normas y recomendaciones desde la triple óptica técnica, organizativa y jurídica, y cuyo cumplimiento implique mediante una acreditación que dicha organización mantiene una infraestructura y un esquema de funcionamiento que garantizan la seguridad de la información que maneja.

Esta norma tiene su origen en el British Standard BS 7799. Esta norma británica está constituida por un código de buenas prácticas y un conjunto de controles o requerimientos que han sido adoptados por numerosas empresas a nivel mundial con el objeto de conseguir una certificación en seguridad de la información por parte de BSI (British Standard Institute) a través de la cual pueden acreditar frente a terceros (clientes, proveedores, etc.) que la empresa maneja su información de forma segura, fijándose de este modo un criterio que determina la confianza en la entidad. La primera parte del BS 7799 (part. I) fue propuesta como un estándar ISO en octubre de 1999. Su aprobación se produjo en octubre del año siguiente, de forma tal que en diciembre del año 2000 fue publicado el ISO/IEC 17799. Esta norma constituye un código de buenas prácticas sin que sea posible obtener una certificación en base a sus disposiciones, puesto que todavía no ha sido aprobado la segunda parte de esta norma ISO.

En España se tomó la iniciativa de desarrollar una norma a través de la cuál, las empresas españolas puedan obtener una certificado similar al del BSI. En este sentido, el organismo encargado de desarrollar una norma equivalente al ISO/ IEC 17799 en nuestro país es AENOR a través del Subcomité 27 de Seguridad de la Información, dependiente del Comité Técnico de Normalización (CTN 71). De este modo, en diciembre del 2002 fue publicada la UNE 71501, esta primera parte es el fiel reflejo de la BS 7799 (Part 1) y de la ISO / IEC 17799 (Parte I), constituyendo en sí misma un código de buenas prácticas cuyo objetivo es servir como instrumento a las empresas para gestionar la seguridad de la información.

Para que las empresas puedan ser certificadas sobre la base de estos códigos de buenas prácticas es preciso el establecimiento de una norma que establezca los criterios o especificaciones que deben reunir los sistemas de gestión de la seguridad de la información (SGSI). Nuevamente, Gran Bretaña fue la pionera publicando la BS 7799 (part. 2) que establece los criterios que debe reunir un SGSI para ser certificable. En Europa, el proceso va más lento y se espera que la ISO /IEC 17799 (Parte II) vea la luz a lo largo del 2007. En lo que se refiere a España, el 23 de junio de 2003, en reunión extraordinaria del Subcomité 27 se aprobó la UNE 71502 “Especificaciones para los sistemas de gestión de la seguridad de la información”, decisión que fue ratificada por el CTN 71. Tras pasar por el correspondiente trámite de información pública y haber resuelto los comentarios el Subcomité 27 fue aprobada definitivamente por el CTN y editada definitivamente por AENOR, en febrero de 2004.

Por tanto actualmente, España al igual que Gran Bretaña cuenta con una norma certificable (UNE 71502), de tal forma que cualquier empresa, que lo desee ya que el sometimiento a los requerimientos que se establecen es voluntario, podrá someterse a los procedimientos fijados para obtener un certificado en materia de gestión de la seguridad de la información, en el que al igual que ocurre en cuanto a calidad, con la norma ISO 9001 constituirá una garantía frente a terceros de que ésta establece unos controles y medidas suficientes, tanto legales, como organizativas y técnicas para mantener la

confidencialidad, integridad y disponibilidad de toda la información que es manejada dentro de la entidad. El objeto de esta norma es establecer las especificaciones para que una empresa desarrolle un SGSI que pueda ser certificado por una entidad independiente.

La norma básicamente comprende los siguientes aspectos.
Política de Seguridad
Organización de la Seguridad
Clasificación y control de activos de información
Gestión de la Seguridad de la información y el personal
Seguridad física y del entorno
Gestión de comunicaciones y operaciones
Control de acceso
Mantenimiento y desarrollo de sistemas
Gestión de la Continuidad del negocio
Conformidad

A la hora de que una empresa decida guiar la gestión de la seguridad de la información sobre los postulados de esta norma en primer lugar deberá llevar a cabo una labor de consultoría tendente a que la entidad cumpla con los parámetros que fija la norma. Para ello deberá en líneas generales:

Definir el alcance del SGSI, es decir sobre qué proceso o procesos va a actuar ya que no es necesario la aplicación de la norma a toda la entidad.
Identificar los activos de información.
Realizar un análisis de riesgos, el cual determinará las amenazas y vulnerabilidades de los activos de información previamente inventariados.
Selección de controles
Determinar, bajo el principio de proporcionalidad, las medidas correctoras a adoptar para disminuir las deficiencias o anomalías detectadas.
Generar la documentación: Política de Seguridad, procedimientos básicos de gestión de la seguridad de la información, protocolos de actuación, registros etc.

Una vez que la empresa ha realizado todas las actuaciones tendentes al cumplimiento de las recomendaciones establecidas en la norma podrá solicitar, si así lo estima conveniente, a una entidad certificadora que acredite dicho cumplimiento.

Con anterioridad a que las entidades independientes (certificadoras) puedan dictaminar la situación de una empresa en relación a la norma, la Entidad Nacional de Acreditación (ENAC) debe crear un esquema de certificación al que las entidades certificadoras deben someterse. Concretamente, en junio de 2004, ENAC publicó una nota informativa en la que establece que “los criterios de acreditación para certificadores de sistemas de gestión de la seguridad de la información están recogidos en la norma UNE-EN 45012 “Requisitos generales para entidades que realizan la evaluación y certificación de sistemas de la calidad”. (Guía ISO/CEI 62) y en el documento EA-7/03 “Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems”. Este ultimo documento, elaborado por un grupo de trabajo de European Co-operation for Accreditation (EA), recoge explicaciones para la aplicación de la norma EN 45012 en el campo de los Sistemas de Gestión de la Seguridad de la Información (SGSI).” Actualmente, ninguna certificadora está acreditada por ENAC, por tanto los certificados que emiten son propios; no obstante, alguna de las entidad certificadora está acreditada ante BSI puede emitir certificados en materia de gestión de seguridad de la información a la Bs.

Capitulo II Herramientas para la administración de la información

La administración de Información en esta era Tecnológica está caracterizada por una dualidad Por un lado, la tecnología puede ser aplicada para automatizar operaciones de acuerdo a una lógica que poco ha cambiado de un sistema del siglo XIX suplantar el cuerpo humano con Tecnología que habilita el mismo proceso con mayor continuidad y control. Por otro lado, la misma Tecnología genera simultáneamente Información sobre el proceso productivo y administrativo a través de la cual la organización logra su trabajo. Ofrece un mayor nivel de transparencia y profundidad sobre las actividades que habían sido parcialmente o completamente opacas. De esta forma la administración de Información con Tecnología sobrepasa la lógica tradicional de automatización. [15]

Explotando detalles mínimos: Esto forma la base de un "CRM"(*Customer Relationship Management*): Mantener información detallada sobre las preferencias de clientes. A través de esta información las empresas logran diferenciarse de la competencia ("Brand Equity"). Las compañías de aviación y hoteleras ya archivan preferencias del cliente como: secciones de "fumar/no fumar", comida preferida ; los Sistemas de Información de hoy en día lograran ofrecer a empresas que nunca antes habían mantenido contacto *directo* con el consumidor final acceso a este "Brand Equity" , Todo con el valor intrínseco de la información.

Generalizando Ideas: Se dice que la capacidad de crecimiento de una compañía es *G X G*, la habilidad de *Generar* ideas multiplicado por la habilidad de *Generalizar* ideas a lo largo de toda la compañía. Estas ideas generales evitan duplicar información, facilitan la transferencia de conocimiento, y reducen el margen de error en simulaciones de toma de decisiones, este es el tema principal de un "KMS" (Knowledge Management System)

Crear un negocio de Información: IBM genera mayores utilidades prestando servicios de asesoría computacional que a través de ventas de equipo, las

compañías de transporte no sólo rentan los camiones de mudanza, sino vende su conocimiento logístico. Inclusive en otras industrias es con Información como se logra reducir el Inventario y en el proceso reducir la cadena de proveedores, esto es el tema de "SCM" (Supply Chain Management).

Los Modelos más utilizados para Administrar Información hoy en día son los siguientes:

KMS "knowledge Management System"

El conocimiento es de dos tipos. Conocemos el tema nosotros mismos, o sabemos dónde podemos encontrar tal conocimiento Samuel Jonson. La información independientemente de los costos a que haya sido creada, puede ser replicada y compartida a un costo mínimo o nulo. Thomas Jefferson. El problema de clasificación surge cada vez que se habla de una Arquitectura en un KMS ("Knowledge Management System"). Tarde o temprano, alguien indica que no toda la información tiene el mismo valor y se propone una clasificación. Una división puede ser la siguiente:

Datos: La temperatura es 90 grados.

Información: Los datos son puestos en contexto: Es una temperatura alta para este tiempo del año.

Conocimiento: Una conclusión que surge a partir de la información: Esta temperatura ambiental presenta un mayor problema del que pensábamos para la nueva planta.

Sabiduría: Todos hablan del clima, pero nadie hace nada por él, se debe hacer exceso de Información.

El depósito de información puede facilitar la resolución de un problema pero a la vez lo puede entorpecer aún más con información trivial y como cualquier otro recurso: "el exceso no es bueno".

Los Detalles de Implementación en un KMS

Las compañías de consultoría que viven o mueren compartiendo su información han invertido millones en estas áreas: Andersen Consulting (hoy en día Accenture): "Knowledge Xchange", Booz Allen & Hamilton "KOL--Knowledge On-line", Cap Gemini Ernst & Young "Center for Business

Knowledge", KPMG "Knowledge Manager", Price Waterhouse "Knowledge View", y la lista continua.

Capital Estructural: Si observamos los estados financieros de una compañía como Microsoft, se observa muy poco "Capital", su valor se encuentra en lo intangible "Capital Estructural", su Sistema de Información " diferencia" e "informa" al personal dentro de la misma empresa, los estados financieros no muestran el valor de los programadores de la corporación, el Jefe de Finanzas sabe cuánto es la nomina, pero no puede estimar cual es el costo de reposición de un empleado, mucho menos si este se está depreciando o apreciando. El director de Recursos Humanos sabe cuánto fue la inversión en cursos de entrenamiento, pero no puede saber cuánto aprendizaje resulto de estas acciones. Sobre esto capitaliza Microsoft, a pesar de ser intangible la diferenciación y el informar es lo que hace que Microsoft sea una empresa valiosa.

Automatizar: Aunque es lo mínimo esperado de un Sistema de Información, esta automatización puede ser aplicada para sustituir varias operaciones en las empresas, (un ejemplo claro antes mencionado) las aerolíneas a través de aplicaciones de servidor que eficiente sus procesos, automatizando a las agencias de viajes.

SCM "Supply Chain Management"

Uno de los principales problemas que afronta cualquier empresa que desee entrar al mercado de Internet es trabajar de una forma eficiente con la cadena de distribución en su Industria, ya sea en un mercado vertical u horizontal, y un aspecto fundamental para aplicarlo es saber diferenciar entre el flujo físico de bienes del flujo de información.

Reconocer la Información: En las industrias clásicas ("Brick and Mortar") estas dos áreas suelen ser integradas en un flujo indivisible, sin embargo, cualquier empresa que aspire a conquistar un mercado en Internet debe saber dividir estas dos áreas. La información empieza a cobrar vida; se convierte, paradójicamente, tan tangible como los productos materiales a los que estamos

acostumbrados, pero para poner esto en contexto sería mejor un ejemplo de la falta de división entre información y el producto físico.

Inventarios: A través de la Historia de los negocios, el inventario derrotaba la información, en gran parte porque la información no podía ser lo suficientemente precisa. Las compañías ocultaban su ignorancia del mercado manteniendo inventario adicional. Los japonenses fueron los primeros en tener eficiencia este proceso en la Industria manufacturera y lo denominaron: *kanban*.

El sistema *kanban* es simplemente un pedazo de papel y tarjetas con un índice de artículos, cuando la línea de producción nota una baja de inventario se anexa éste papel a un red de "hilo" solicitando más partes, esto es todo lo que realiza *kanban* hoy en día esta metodología *kanban* es utilizada en una red gigantesca de proveedores, del "hilo" utilizado en la línea de producción hasta la Red de Telefonía privada o pública (Internet); nadie mantiene mayor inventario del necesario, *información en tiempo real* suple al inventario.

El Fin del Inventario: Conforme la importancia de la información continua, seguirán surgiendo compañías que su principal recurso será la información, las compañías desearan menos el capital físico y se convertirán en solo información. La diferencia en la estructura financiera de un compañía que solo utiliza Información puede ser tan diferente de una Industria con bienes tangibles, que en ocasiones es incomprensible.

Cadena de Distribución ("Supply Chain") en Tiempo Real

Porque esta afinidad hacia la información Permite tener un *conocimiento y control* sin precedente sobre las operaciones de una empresa. A continuación se menciona como puede ser logrado este control en diversas áreas de una cadena de distribución.

2.1 La información como ventaja competitiva de las organizaciones

La competitividad de una empresa se puede definir como su habilidad o capacidad para competir con otras firmas, es decir, su capacidad para luchar favorablemente en un mercado. Esta capacidad se traduce en la obtención o desarrollo de ventajas de la empresa respecto a sus competidores y, en último extremo, en el hecho de que los clientes perciban como más ventajoso adquirir productos de la empresa en cuestión que adquirir los de sus competidores. [17]

Una empresa puede conseguir ventajas competitivas de tres formas principales:

1. Consiguiendo un liderazgo de costes: el cual trata de que los costes de concepción, desarrollo, manufacturación o distribución del producto sean menores que los correspondientes costes de los competidores, de manera que el coste final por unidad producida sea inferior y permita establecer un precio del producto también inferior. Las dos estrategias principales para conseguir menores costes son la reducción o eliminación de todo lo inútil o superfluo del proceso de producción y la mejora o incremento de la productividad.
2. Diferenciando sus productos de los de la competencia: La empresa consigue ventajas competitivas añadiendo características únicas al producto, de forma que por un mismo precio se ofrecen más prestaciones que los correspondientes productos de la competencia.
3. Consiguiendo (y dominando) un nicho de mercado: El producto se dirige a un sector del mercado muy concreto, que intenta explotar en régimen de exclusividad.

Se ha visto entonces que las tecnologías de información se han aplicado tradicionalmente con el objetivo básico de reducir costes y aumentar la productividad, generalmente a través de la automatización de operaciones internas (es decir, a través de la implantación de sistemas tácticos). En este sentido, las TI han contribuido a aumentar la competitividad de las empresas porque han incidido directamente sobre una de las estrategias tradicionales de competitividad (liderazgo de costes).

2.2 El valor de la información

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: es un activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- Protección a la Réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

- No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

- Aislamiento: este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.[18]

2.3 Seguridad de la información y gestión de riesgos

La seguridad de la información se ha convertido en una cuestión prioritaria para las grandes organizaciones con operaciones sofisticadas de seguridad. Las amenazas continúan surgiendo, los sistemas evolucionan y la gente desea sacarle más provecho a las redes.

Los problemas de seguridad pueden dar como resultado menores ingresos, mayores gastos y sanciones adicionales o la erosión de la confianza y el control informático con el tiempo. Las herramientas de supervisión de la red para identificar los puntos o vulnerabilidades de los ataques técnicos ayudan a identificar los problemas técnicos. Sin embargo, las personas y los procesos pueden comprometer los controles técnicos por medio de un uso indebido accidental o intencionado, poniendo en riesgo la información y las redes.

Un método exhaustivo de gestión de riesgos para la seguridad de la información requiere la identificación de las vulnerabilidades y amenazas que tienen más probabilidad de producirse, la cuantificación del daño potencial a su negocio y el desarrollo de esfuerzos de mitigación para lograr un nivel de riesgo aceptable. No sólo es gestionar un dispositivo, introducir un cambio de reglas o corregir un nivel de colocación de parches. Requiere determinar que a activos se deben colocar primero los parches, qué controles se deben implementar, y si se produce o no la colocación de parches, qué efecto tendrán los esfuerzos de solución en la exposición general al riesgo.

El proceso de gestión de riesgos comienza con el desarrollo de un informe de gestión de riesgos que incluya una declaración de tolerancia de riesgo aceptable utilizada para determinar las políticas y comunicar las decisiones a los participantes.

El proceso de identificación de riesgos utiliza datos en tiempo real para identificar las vulnerabilidades y amenazas relacionadas con la tecnología, las personas y los procesos de seguridad.

La aplicación de los marcos de evaluación de estándar, como ISO 17799 y BSI 7799-2, en el informe de gestión de riesgos y la identificación de riesgos muestra cómo las políticas de empresa y la implementación se adecuan al código ético de la seguridad internacional.

A través del análisis de riesgos y las amenazas potenciales, se identifican y cuantifican, según la probabilidad de ataque, el valor del activo para el negocio, la ubicación del activo en la red y cualquier asunto legal o de cumplimiento normativo relacionado con el riesgo. El análisis de riesgos ayuda a las empresas a dar prioridad a los riesgos y optimizar los recursos disponibles.

El plan de respuesta y el plan de mitigación de riesgos dan prioridad a las acciones que reducen el riesgo con la mayor brevedad y eficacia de costes posible.

La evaluación regular y la supervisión continua ayudan a asegurar que la mitigación ha tenido lugar y a identificar nuevas amenazas, mejora del rendimiento de seguridad

Al cambiar las condiciones y sistemas, los profesionales de la seguridad realizan compensaciones para lograr un nivel aceptable de riesgo sin comprometer la disponibilidad, confidencialidad e integridad de los datos. Un programa de gestión de riesgos eficaz ofrece a los altos ejecutivos una forma de gestionar la evolución de los sistemas de seguridad de la información. [19]

2.5 Protección de la información

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

A. La Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

B. La Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

C. La Recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

El Daño es el resultado de la amenaza; aunque esto es sólo la mitad de la sentencia. El daño también es el resultado de la no–acción, o acción

defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

El protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las Contramedidas (técnicas de protección) adecuadas. La Seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de Fiabilidad y se la define como “la probabilidad de que un sistema se comporte tal y como se espera de él”6, y se habla de Sistema Fiable en vez de sistema seguro.

Para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer “qué es lo que queremos proteger”, “de quién lo queremos proteger”, “cómo se puede lograr esto legislativa y técnicamente”; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución (¿anulación?) de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que no existe el 100% de seguridad esperado o deseable en estas circunstancias. [20]

Capitulo lll Caso de Aplicación Metodología Magerit

Introducción

El CSAE (Consejo Superior de Administración Electrónica.) ha elaborado y promueve Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) como respuesta a la percepción de que la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

Pese a que se ha puesto en manos de los sistemas de información graves responsabilidades para cumplir los objetivos de las organizaciones, no deja de ser un tema recurrente la inquietud por su seguridad. Los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y sobre todo cuando la inversión en defensa de los medios de trabajo no se traduce en la ausencia de fallos. Lo ideal es que los sistemas no fallen. Pero lo cierto que se acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes como la confianza de que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

3.1 Objetivos de Magerit

1. hacer conciencia a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo
2. ofrecer un método sistemático para analizar tales riesgos
3. ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control
4. preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

3.2 Realización del análisis y de la gestión

Hay dos grandes tareas a realizar:

I. Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

Elementos:

1. activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización
2. amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen tanto daño.

Con estos elementos se puede estimar:

1. el impacto: lo que podría pasar
2. el riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

II. gestión de riesgos, que permite organizar la defensa cuidadosa y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

3.3 Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza de forma que las estimaciones de impacto y riesgo sean “potenciales”.

Activos

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.

Las aplicaciones informáticas (software) que permiten manejar los datos.

Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.

Los soportes de información que son dispositivos de almacenamiento de datos.

El equipamiento auxiliar que complementa el material informático.

Las redes de comunicaciones que permiten intercambiar datos.

Las instalaciones que acogen equipos informáticos y de comunicaciones.

Las personas que explotan u operan todos los elementos anteriormente citados.

Tipos de activos

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes

Si el sistema maneja datos de carácter personal, estos suelen ser importantes por sí mismos y requerir una serie de salvaguardas frecuentemente reguladas por ley. En estos activos interesa

Determinar qué tratamiento hay que imponerles. El hecho de que un dato sea de carácter personal impacta sobre todos los activos involucrados en su tratamiento y custodia.

Algo similar ocurre con los datos sometidos a una clasificación de confidencialidad. Cuando se dice que un cierto informe está clasificado como “reservado”, de forma que las copias están numeradas, sólo pueden llegar a ciertas personas, no deben salir del recinto y deben ser destruidas concienzudamente, etc. se están imponiendo una serie de salvaguardas porque lo ordena el reglamento, sectorial o específico de la Organización.

Dependencias.

Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos más materiales como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. Por ello aparece como importante el concepto de “dependencias entre activos” o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores: capa 1: el entorno: activos que se precisan para garantizar las siguientes capas equipamiento y suministros:

energía, climatización, comunicaciones personal: de dirección, de operación, de desarrollo, etc. Otros: edificios, mobiliario, etc. Capa 2: el sistema de información propiamente dicho equipos informáticos (hardware) aplicaciones (software) comunicaciones soportes de información: discos, cintas, etc. la información datos meta-datos: estructuras, índices, claves de cifra, etc. Capa 3 las funciones de la Organización, que justifican la existencia del sistema de información y le dan finalidad objetivos y misión bienes y servicios producidos capa 4: otros activos

Es como si el legislador hubiera realizado el análisis de riesgos por nosotros y hubiera determinado las salvaguardas pertinentes. En todo caso, leyes y regulaciones existen y ayudan a que estos datos, ciertamente importantes, estén protegidos.

Un ejemplo puede ser mejor que mil palabras. Si se quema el local que hospeda los equipos, lo que no funciona es el servicio percibido por el usuario a kilómetros de distancia. Si roban el portátil de un ejecutivo con información estratégica de la empresa, lo que sufre es la confidencialidad de dicha información.

Las instalaciones se reconstruyen; pero puede haberse pasado la oportunidad de prestar el servicio. El robo se subsana comprando otro portátil; pero el secreto ya está perdido.

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Por otra parte, los sistemas de información

explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de datos y servicios finales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones: su autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar) su confidencialidad: ¿qué daño causaría que lo conociera quien no debe?

Esta valoración es típica de datos. Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?

Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falso o, incluso, faltar datos. Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

Esta valoración es típica de los servicios

En sistemas dedicados a la administración electrónica o al comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. En estos activos, además de la autenticidad, interesa calibrar la: la trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo? La trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Hay servicios finales que materializan la misión última de la Organización. Hay servicios internos de los que la Organización se sirve para estructurar su propia

distribución de responsabilidades. Por último, hay servicios que se adquieren de otras organizaciones: suministros externos.

Realización del análisis y gestión se reconocen habitualmente las dimensiones básicas: autenticidad, confidencialidad, integridad y disponibilidad. En esta metodología se ha refinado la autenticidad para distinguir entre el uso de un servicio y el acceso a unos datos. Además se ha introducido el concepto de trazabilidad (del inglés, accountability) tomado de las guías ISO/IEC 13335, igualmente segmentada entra la trazabilidad del servicio y la de los datos. Los aspectos de autenticidad y trazabilidad de los datos son críticos para satisfacer medidas reglamentarias sobre ficheros que contengan datos de carácter personal.

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es dificultad para que también puedan merecer, adicionalmente, su valoración propia.

¿Cuánto vale la “salud” de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría salir de una incidencia que destrozara el activo. Hay muchos factores a considerar: coste de reposición: adquisición e instalación coste de mano de obra (especializada) invertida en recuperar (el valor) del activo lucro cesante: pérdida de ingresos capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas sanciones por incumplimiento de la ley u obligaciones contractuales daño a otros activos, propios o ajenos daño a personas daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son: la homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una

dimensión o en otra la relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos

Todos estos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para

"curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente.

Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.) pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero no adolecen de los problemas de las valoraciones cualitativas. Sumar valores numéricos es absolutamente "natural" y la interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas: ¿Vale la pena invertir tanto dinero en esta salvaguarda? ¿Qué conjunto de salvaguardas optimizan la inversión? ¿En qué plazo de tiempo se recupera la inversión? ¿Cuánto es razonable que cueste la prima de un seguro?

El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

En consecuencia, para valorar la [interrupción de la] disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como el siguiente: coste de la interrupción de la disponibilidad

Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Hay accidentes naturales (terremotos, inundaciones) y desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

No todas las amenazas afectan a todos los activos de activo y lo que le podría ocurrir.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos: degradación: cuán perjudicado resultaría el activo frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde.

Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

Pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

Las instalaciones pueden incendiarse; pero las aplicaciones, no. Las personas pueden ser objeto de un ataque bacteriológico; pero los servicios, no. Sin embargo, los virus informáticos afectan a las aplicaciones, no a las personas.

Se mide como el número medio de ocurrencias de la amenaza en un intervalo determinado de tiempo.

Típicamente estima sobre periodos anuales. Por ejemplo, si en un cierto sistema se produce una avería.

Determinación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta su valor acumulado (el propio mas el acumulado de los activos que dependen de él) las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta su valor propio las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden

agregarse bajo ciertas condiciones: puede agregarse el impacto repercutido sobre diferentes activos, puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común, no debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores, puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,

Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia.

El riesgo crece con el impacto y con la frecuencia.

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que ofrecer a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la

misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones: Puede agregarse el riesgo repercutido sobre diferentes activos, puede agregarse el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común, no debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores, puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes, puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la frecuencia de las amenazas.

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que: es teóricamente idónea está perfectamente desplegada, configurada y mantenida se emplea siempre existen procedimientos claros de uso normal y en caso de incidencias los usuarios están formados y concienciados existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

Revisión impacto residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Revisión del paso 5: riesgo residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Gestión de Riesgos

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable.

Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

La interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias.

Los párrafos siguientes se refieren conjuntamente a impacto y riesgo.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza

Don Quijote (Capítulo X) llamaba la atención sobre el “bálsamo de Fierabrás” que “es un bálsamo con el cual no hay que tener temor a la muerte, ni hay pensar morir de ferida alguna. “ No puede el responsable de seguridad caer en la confianza ciega pues los sistemas evolucionan, los atacantes inventan, los

Mientras el valor residual sea más que despreciable, hay una cierta exposición.
Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias.

Selección de salvaguardas

Las amenazas hay que pedirlas, por principio y mientras no se justifique lo contrario.

Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa
2. establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
3. establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer
4. desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas

5. desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto A este conjunto de elementos se le encasilla habitualmente bajo el nombre de

Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

El párrafo anterior puede llamar a engaño si el lector interpreta que hay que llevar a cabo todos y cada uno de los puntos para cada amenaza. No. En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí, verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más “abierto” es el de determinación de las salvaguardas apropiadas.

Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la literatura y basta elegir de entre un catálogo en función de la magnitud del riesgo.

Tipos de salvaguardas

Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable. Es decir, impedir incidentes o ataques.

En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes. Tanto para enfrentar lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre.

Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos.

Usuarios son impredecibles en sus errores y en definitiva siempre hay que estar atento y pronto a reaccionar ante nuevas realidades.

Es de sentido común intentar actuar de forma preventiva para que las cosas no puedan ocurrir o no puedan causar mucho daño; pero no siempre es posible y

hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar.

Por último, sin ánimo de saturar al lector, hay que recordar que conviene llegar a un cierto equilibrio entre salvaguardas técnicas: en aplicaciones, equipos y comunicaciones salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos medidas de organización: de prevención y gestión de las incidencias política de personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado: polí-tica de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

Pérdidas y ganancias

Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a proteger.

Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la in-seguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

Hay que entender si la única consideración es económica.

Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni o la parte del cálculo del coste de las salvaguardas. En otras palabras, la curva anterior es conceptual y no se puede dibujar en un caso real.

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

E0: si no se hace nada

E1: si se aplica un cierto conjunto de salvaguardas

E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (no hacer nada) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero. Considerando los siguientes componentes: (recurrente) riesgo residual (una vez) coste de las salvaguardas (recurrente) coste anual de mantenimiento de las salvaguardas + (recurrente) mejora en la productividad + (recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año.

En E0 se sabe lo que cada año (se estima que) se pierde El escenario E1 aparece como mala idea, pues supone un gasto añadido el primer año; pero este gasto no se recupera en años venideros. No así el escenario E2 que, suponiendo un mayor desembolso inicial, empieza a ser rentable a partir del cuarto año. Más atractivo aún es el escenario E3 en el que a costa de un mayor desembolso inicial, se empieza a ahorrar al tercer año, e incluso se llega a obtener beneficios operativos a partir del quinto año. Se puede decir que en escenario E3 se ha hecho una buena inversión.

La actitud de la Dirección

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección Si el impacto y/o el riesgo están por encima de lo aceptable, se puede:

1. eliminar el activo; suena muy fuerte, pero a veces hay activos que, simplemente, no vale la pena mantener
2. introducir nuevas salvaguardas o mejorar la eficacia de las presentes

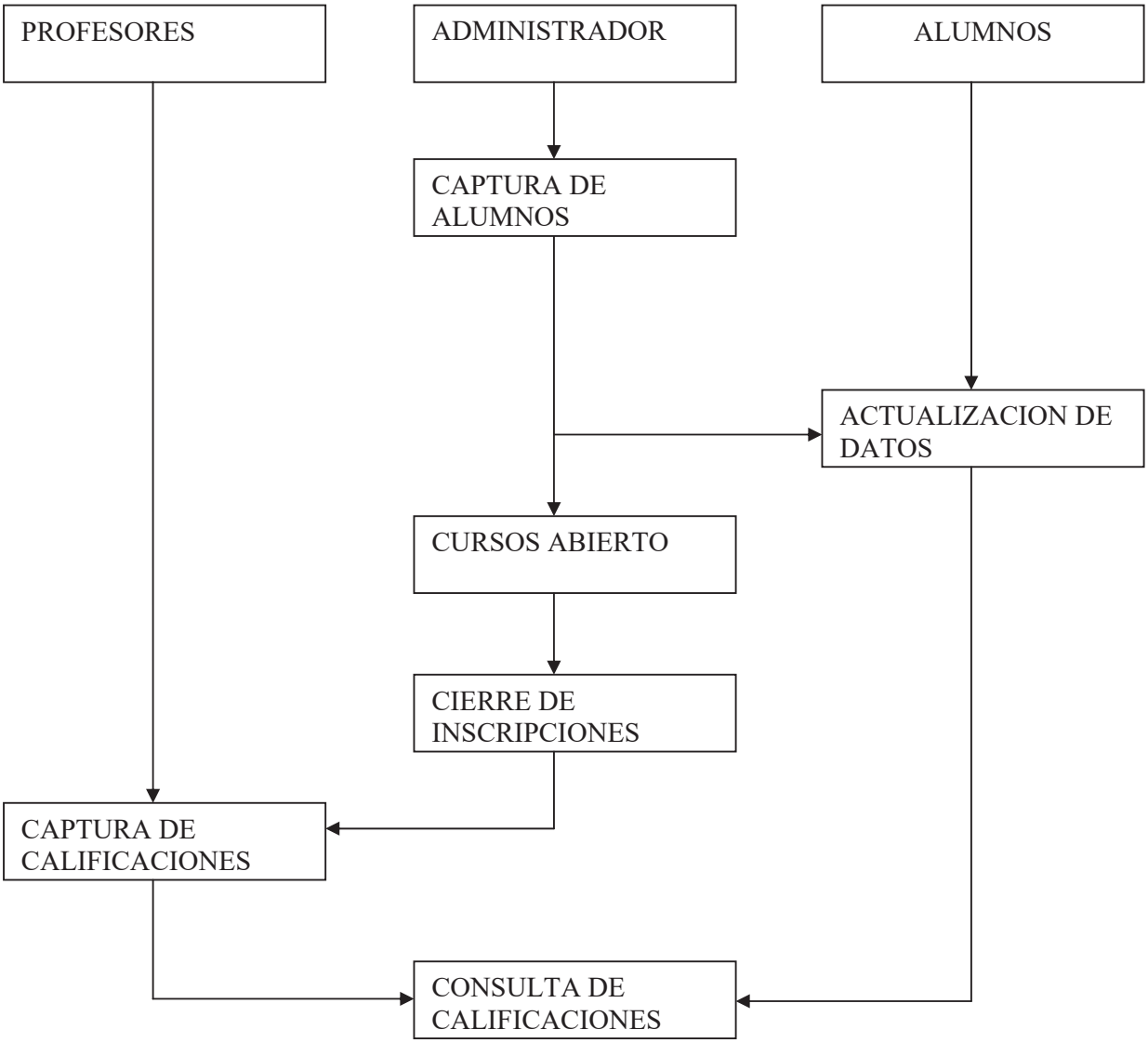
Hablar de Dirección es pecar de simplificar la realidad. Porque al final si se aceptan riesgos imprudentemente elevados, el perjudicado puede no ser sólo el que dirige, sino todos los que tienen su confianza puesta en la Organización y cuyo lamentable desempeño oscurecería sus legítimas expectativas. En última instancia puede verse afectada la confianza en un sector o en una tecnología por la imprudente puesta en escena de algunos actores.
¿Necesita realmente mantener este dato de carácter personal y nivel alto? ¿Es realmente necesaria la red inalámbrica en la oficina?

Revisión de activos
Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valor del sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor. Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

3.4 Aplicación de Caso Práctico

En el caso práctico se mostrara la *Metodología Magerit*, para la utilización de una buena administración de la información en una organización, se detallara los fines de dicha metodología para su aplicación y paso a paso como se debe realizar cada actividad en caso de que sea necesario, esta metodología es muy extensa por lo que únicamente se mostrara la fase de la realización de análisis y la gestión de riesgos.

PROCESO DEL SISTEMA KARDEX



Captura de alumnos: El administrador realiza la captura de cada alumno con su respectiva matricula.

Actualización de datos: Cada alumno realizara su activación de cuenta posteriormente podrá tener accesos a los cursos.

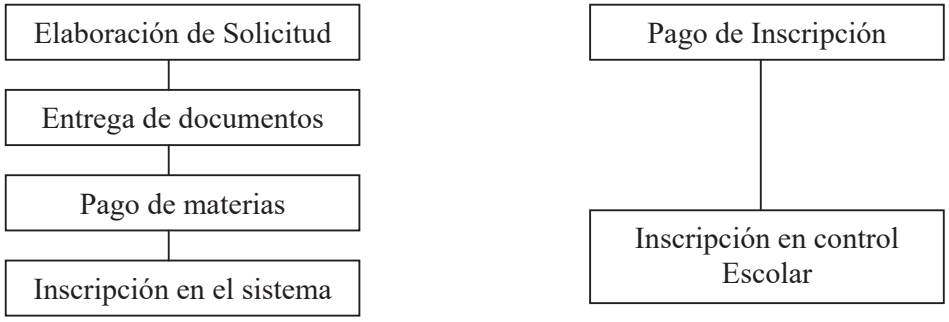
Cursos abiertos: En esta sección el alumno podrá seleccionar los cursos que desea tomar, se establece un control jerárquico para las materias y un cupo.

Cierre de preinscripciones: No se permite el acceso de inscripción a cursos, se cambia el estatus, puedes consultar tus materias elegidas para cursar.

Captura de calificaciones: En esta sección el profesor procederá a dar de alta las calificaciones obtenidas durante el curso, se tiene un tiempo para estatus. Después se procede cerrar.

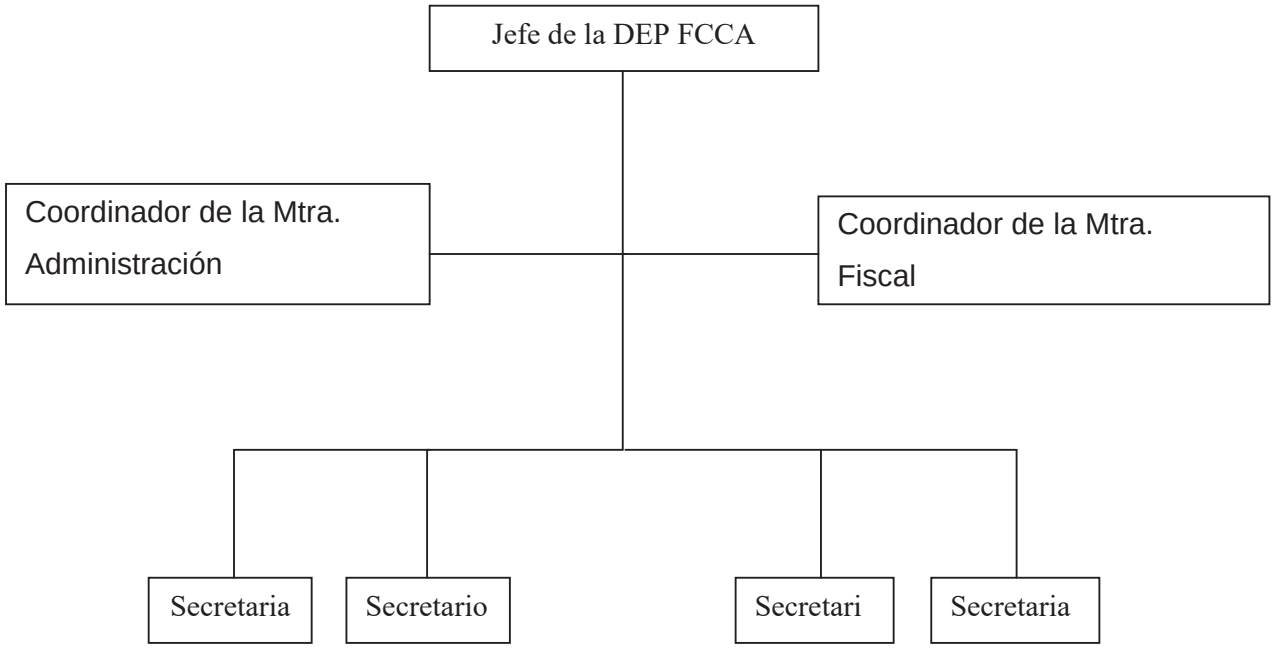
Consultar calificación: El alumno podrá consultar sus calificaciones y el avance que lleva respecto a la maestría.

PROCESO DEL AREA DE POSGRADO



El trámite de inscripción oficialmente se realiza en control escolar, sin embargo en el departamento de posgrado se realizan todos los ajustes tanto para la convocatoria como la asignación de materias que pueden cursar, dudas aclaraciones sobre la maestría que estén cursando.

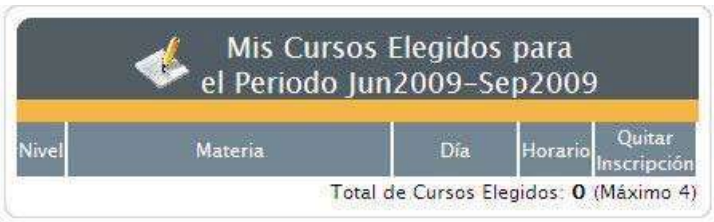
Jerarquía Administrativa



Inicio al sistema de kardex, existen dos tipo de sesiones alumnos y profesores

Consulta de materias cursadas y promedio obtenido

Cursos disponibles para inscripción.



Nivel	Materia	Día	Horario	Lugares Disponibles	Inscribir
0	COMPUTACION	JUEVES	18:30 a 21:30 Hrs	0	LLENO
0	CONTABILIDAD	VIERNES	18:30 a 21:30 Hrs	0	LLENO
0	INGLES	MARTES	18:30 a 21:30 Hrs	7	
0	INGLES		00:00 a 00:00 Hrs	6	
0	MATEMATICAS	MIERCOLES	18:30 a 21:30 Hrs	0	LLENO
1	ANALISIS CUANTITATIVOS	MARTES	18:30 a 22:30 Hrs	0	LLENO

Alta de profesores

Captura de calificaciones.

MODELO DE VALOR: La información que administra el sistema nos permite seguir un proceso de inscripción más rápido (la facultad depende de esa información para ingresos de alumnos, administración de datos, proceso de inscripción a la maestría, servicio al alumno), que objetivos persigue (rapidez en el servicio de inscripción a la maestría, control y eficiencia de información), cuáles son sus objetivos principales dependencia la información (la información del alumno nos lleva, asignar cursos, de ahí dependerá su historial para terminar sus estudios, la perdida de cualquiera de las anteriores nos llevaría a la pérdida total de la información, si tenemos un control de sus material cursadas, pero si no existen calificaciones su expediente será incompleto)

- ✓ Dentro del modelo de valor el personal y el área administrativa esta consientes de lo que vale dicha información para llevar a cabo su

proceso, sin embargo es necesario tomar en cuenta el reflejar eso en el momento de brindar el servicio a los alumnos, el mejorar el sistema para un trámite más ágil sería muy útil para el alumno como para el personal.

MAPA DE RIESGO: Que tipo de amenazas existen:

- Robo de información (extraer información para fines para los cuales no fue diseñada),
- Información falsa (modificación de datos reales)
- Mala administración (falta de mantenimiento al sistema, descuido en el proceso, poco interés por parte de los directivos),
- Un servicio incompetente (que el usuario este inconformes por el proceso que realizan).

EVALUACION DE SALVAGUARDAS: Tiene una eficiencia de un 80%, permite realizar un proceso, pero carece de efectividad en selección de materias, no cuenta con las normas establecidas para asignación de dichas materias, la seguridad establecida para el servidor que administra el sistema de kardex es buena, la realización de respaldos es pobre, ello nos lleva a posible pérdida de información, en relación al riesgo existen medidas en caso de cambio de datos, ejemplo: las calificaciones incorrectas se dan de baja por el administrador y se vuelven a capturar aun después de haber cerrado el status de captura de calificaciones, esto únicamente por el administrador.

- ✓ Deberían existir salvaguardas más efectivas y que la aplicación de estas sea con menos esfuerzos, la realización de respaldos podría fijarse tomando en cuenta las operaciones de trabajo ejemplo, respaldar cuando se cierra el proceso, así no sería necesario estar respaldando semanalmente, esto nos evitaría trabajo y tendríamos seguridad.

ESTADO DE RIESGO:

- Que puede llegar a ocurrir (duplicidad de contraseñas, se realiza cambio de contraseña a la semana del administrador)

- Manipulación del sistema (existen respaldo que se realizan para almacenamiento de información, pero no se actualizan, ni se tiene un control para su realización).
- Si existe una mala administración (no existen personal auxiliar para supervisar el control de la administración del sistema, no se continuo con el mantenimiento necesario para continuidad del sistema kardex)

✓ Tomando en cuenta lo anterior podemos base a resultados mejorar nuestros estados de riesgos ejemplo, no es tan necesario realizar cambio de contraseñas semanalmente cuando el sistema está en consulta de información, ahora cuando se está en captura de calificaciones si sería importante por el hecho de que diariamente se está subiendo información.

INFORME DE INSUFICIENCIAS: No existe seguridad para software malicioso para la obtención de contraseñas, no tiene un control de que debilidad tiene la seguridad que se le establece, no es visible detectar intrusos en el sistema, no se construyo el sistema con el tiempo necesario debido a la necesidad de utilizarlo, existen procesos que aun no se terminan de concluir.

PLAN DE SEGURIDAD: No existe solo se cuenta con algunos respaldos y la información está en archivo.

✓ Concluir los procesos a realizar para en buen funcionamiento del sistema, esto nos garantizara un poco mas de confianza, involucrar a más personal para su administración, aplicación de seguridad para las contraseñas, supervisión de los procesos.

REALIZACION DEL ANALISIS Y DE LA GESTION

ANALISIS DE RIESGOS: Se cuenta con información de cada alumno, control de materias cursadas e información personal en algunos casos

ACTIVOS: Equipo de computo disponible para el buen funcionamiento del sistema kardex (información, servicios, aplicaciones, personal,)

AMENAZAS: En caso de pérdida de la información la afectación que tendrá la facultad será volver al proceso de inicio, más largo y tardado la inscripción, mientras se repara la base de datos.
SALVAGUARDAS: Cuenta con respaldos, existe otro tipo de almacenamiento de la información (boletas de calificaciones)

- IMPACTO: Consecuencias posibles a realizar (pérdida total, parcial)
- EL RIESGO: Que ocurrirá cuando pase eso.

Estado del riesgo: Por lo que pueda pasar tomando las salvaguardas, ejemplo. En caso de conocimiento de claves administrativas, se cambia por otra, esta se está cambiando por seguridad.

GESTION DE RIESGOS: Medidas a tomar por la dirección en caso de afectación, opciones que se tiene para un mejor control de la situación. Mejorara el proceso tomando en cuentas todo lo anterior para brindar un mejor servicio y mayor seguridad.

- ✓ Dentro del análisis y la gestión podemos corroborar lo ya mencionado, la escases en cuestión de salvaguardas, tener conciencia del impacto que esto nos provocaría, al involucrar más al personal con el sistemas podemos evitar riesgos, se asegura que si existen daños podemos fácilmente ver la solución, y saber que ya tenemos la solución para cuando acurra, nos da seguridad y confianza para su utilización.

PROCESOS DE INVESTIGACION
Análisis del funcionamiento del sistema: En la primera fase se llevo la tarea de revisar que era realmente lo que el sistema nos brindaba como servicio a los alumnos.

Entrevistas: La realización de ellas me permitió ver la disponibilidad del personal para cambios en el sistema y la importancia que le dan al sistema como una herramienta en su trabajo.

Realización de cuestionarios: se realizaron para tener más seguridad sobre el funcionamiento del proceso de inscripción y poder hacer una comparación sobre lo que hace y lo que podría hacer.

Análisis de los procesos administrativos para ingreso al posgrado

PROPUESTA DE MEJORA (en cada punto tomar una propuesta de mejora)

- Continuidad con el Mantenimiento del sistema
  Es importante que si se brinda un servicio se realice con la mayor satisfacción y que garantice la mayor seguridad.
- Asignación de personal para el buen manejo de kardex
  Es más fácil trabajar si se nos especializa en algo, y se trabaja mejor si se nos responsabiliza de lo que hacemos.
- Ver implantación de normas del procesos de inscripción
  Tomar en cuenta las normas y procesos que lleva la facultad para no duplicar trabajo.
- Ver implantación de normas del procesos de inscripción

CONCLUSIONES

1.La metodología utilizada para el maneo de la información conocida como Magerit, nos permite identificar puntos clave para la utilización de nuestra información en el sistema kardex, nos permite métodos sistemáticos para el análisis del riesgo y sus consecuencias posibles, nos lleva a conocer lo que realmente contiene nuestro sistema.

2. Las herramientas utilizadas para la administración de la información, son el valor, el riesgo, la seguridad que le otorgamos a dicho kardex para su buen uso.

3. Los puntos clave para su buena utilización de la información como lo menciona, algunos autores como Diebold es manejada como u recurso

fundamental, Wang Lee, Pipno y Strong es como un producto, en conclusión nos permite brindar un mejor servicio, si tomamos en cuenta la importancia que tiene.

4. Tomando en cuenta la protección que le damos a nuestra información los aspectos más importantes es tener una información que sea confiable, integra y que esté disponible para cuando el alumno lo requiera, y no sea modificada de forma errónea para la cual es requerida.

5. Nuestra información que recibe protección es muy amplia ya que todos los datos que se en cuentan en el sistema kardex son muy importantes empezando desde el nombre, calificaciones, datos personales y hasta la información que se presenta para la utilización del mismo sistema.

6. Nuestros métodos para la seguridad de la información se basan en:

-Buena administración apara el manejo del sistema, tener un proceso del sistema y hacerlo conocer por el personal para involucrarlos mas.

-Evaluar riesgos posibles, establecer salvaguardas en caso de ocurrir, como nos explica la metodología Magerit, es necesario conocer los riesgos para minimizarlos cuando ocurran, no significa que no ocurrirán, pero tenemos una salvaguarda para cuando ocurra.

7. Los cambios que se logran en referencia a tener seguridad en el sistema kardex minimizara el trabajo del personal de posgrado, mejorara el servicio al alumno y sobre todo agilizara el trámite de inscripción a las maestrías.

Se llevo el análisis de metodologías para la administración de información y sus diferentes formas de ver a la información algunos autores la ven como ventaja , lo que si es que en la actualidad las empresas han obtenido algo a cambio de esta, mas sin embargo también se puede decir que aun no se puede ver como algo confiable por la falta de seguridad y por el hecho de no ser un bien tangible.

En el caso práctico se llego a la conclusión que para brindar un buen servicio debemos nosotros mismos confiar primero en lo que estamos comunicando antes de que terceras personas lo hagan, en el sistema del kardex puede observar que ofrece un servicio que permite llevar proceso, sin embargo está

incompleto ya que los alumnos no obtiene toda la información que necesitan, lo cual no satisface el servicio y por consecuencia el trabajo se duplica.

[1] González Teruel, Aurora (2005)

[2] Adaptado por Alfons Cornella del Modelo de Laudon y Laudon [LAUDON, K.C. y LAUDON, J.P. Business Information Systems. Orlando: the Dryden Press, 1991].

[3] CORNELLA, Alfons. Ibid., p. 104-106

[4] PRESTHUS, R. The organizational Society. Nueva York, 1962. Citado en: MOZZELIS, Nicos P. Organización y burocracia. Barcelona: Ediciones Península, 1991, p. 7.

[5] CHAÍN NAVARRO, Celia. Gestión de información p. 45.

[6] (Cornellá, Alfonso, 1994: 78).

[7] (Arias y Portela, 1997).

[8] Alin, Lafont y Macary (1997)

[9] GIL PECHUAN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Madrid: McGraw-Hill, 1997, p. 27-28.

[10] (Hornos, Araque y Abad, 1998: 185)

[11] (Quinn, Anderson y Finkelstein, 1996: 12)

[12] (Escobar, 1997: 31)

[13] (Wang, Lee, Pipino y Strong, 1999: 53)

[14] CHAÍN NAVARRO, Celia. Gestión de información

[15] Shoshana Zuboff, Profesor HBS School

[16] Nexos - Enrique Daltabuit, Seguridad de la información en la actualidad.

[17] María Pilar Segura Bas, subdirectora de Ibercaja

[18] Greenwood, W.T. [1978] "Teoría de decisiones y sistemas de información. Introducción a la toma de decisiones administrativas". México, Editorial Trillas.

[19] Navarro, Carlisle Angulo, Diana García, Ana Luisa. Desarrollo del Sistema de Información Administrativa.
[20] HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital – Open Publication License v.10.

Bibliografía

- González Teruel, Aurora (2005). Los estudios de necesidades y usos de la información: fundamentos y perspectivas actuales. Gijón: Trea.

- Roberto Rebolloso gallardo. La globalización y las nuevas tecnologías de información. Trillas.

- Rias Coello, Alicia y Portela Filgueiras, Isabel. (1997). "Sistema de información y sistema de calidad: relación y dependencia en las organizaciones empresariales, en Documentación de las Ciencias de la Información. Núm. 20. Madrid. ISSN: 0210-4210.

- Chain Navarro Celia, Técnicas y Métodos de Recuperación de Información, Diego Marin.

- Adaptado por Alfons Cornella del Modelo de Laudon y Laudon [LAUDON, K.C. y LAUDON, J.P. Business Information Systems. Orlando: the Dryden Press, 1991].

- PRESTHUS, R. The organizational Society. Nueva York, 1962. Citado en: MOZZELIS, Nicos P. Organización y burocracia. Barcelona: Ediciones Península, 1991, p. 7.

- CORNELLA, ALFONSO. RECURSOS DE INFORMACION. McGraw-Hill/ Interamericana de España

- GIL PECHUAN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Madrid: McGraw-Hill, 1997, p. 27-28.

- Greenwood, W.T. [1978] "Teoría de decisiones y sistemas de información. Introducción a la toma de decisiones administrativas". México, Editorial Trillas.

- Navarro, Carlisle Angulo, Diana García, Ana Luisa. Desarrollo del Sistema de Información Administrativa.

- HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital Open Publication License v.10.

http://monografias.com

http://www.degerencia.com

http://www.ugb.edu.sv

http://www.ull.es/

http://www.edgarvega.cr.gs

http://hbs.edu

http://www.hipertext.net/

http://www.kriptopolis.com

http://publicaciones.administracion.es