Curso:
Administración y Seguridad de Sistemas

Responsable: Ms Ing. Cristina Mayr

Administración

Definición de Administración

1. *Según la American Management Association:*

Guiar o conducir recursos humanos y físicos hacia unidades de organización dinámicas que cumplen sus objetivos (para la satisfacción de aquellos a quienes se sirve) con un alto grado de moral y sentido de realización por parte de aquellos que brindan el servicio.

2. *Otra definición:*

Obtener cosas por intermedio de personas.

3. *Kliksberg:*

“La administración es un conjunto de conocimiento referentes a las organizaciones integradas por nociones atinentes a la explicación científica de su comportamiento y nociones atinentes a su tecnología de conducción".

4. *Valladares Román:*

"La administración, es el proceso para alcanzar resultados positivos a través de una adecuada utilización de los recursos disponibles y la colaboración del esfuerzo ajeno"

5. *Koontz y O¨Donnell:*

"La administración se define como la creación o conservación en una empresa, de un ambiente donde los individuos, trabajando en grupo, pueden desempeñarse eficaz y eficientemente, para la obtención de sus fines comunes".

6. *Henry Sisk y Mario Suerdlik:*

"Es la coordinación de todos los recursos a través del Proceso de Planeación, dirección y control, a fin de lograr objetivos establecido".

7. *Barcos Santiago:*

"La administración como disciplina científica constituye un sistema de conocimientos, metódicamente fundamentado, cuyo objeto de estudio son las organizaciones y la administración – en el sentido de conducción, proceso, gestión de recursos, etc – de éstas"

Si se analizan detenidamente las definiciones, se observa que todos los autores concuerdan, de

una u otra manera, en que el concepto de administración está integrado por los siguientes elementos:

- *Objetivo*: La administración siempre está enfocada a lograr fines o resultados.
- *Eficiencia*: La administración no sólo busca lograr obtener resultados, sino optimizarlas mediante el aprovechamiento de todos los recursos.
- *Grupo Social*: Para que la administración exista es necesario que se dé siempre dentro de un grupo social.
- *Colaboración del esfuerzo ajeno*: La administración aparece precisamente cuando es necesario lograr ciertos resultados a través de la colaboración de otras personas.
- *Coordinación de recursos*: Para administrar, se requiere combinar, sistematizar y analizar los diferentes recursos que intervienen en el logro de un fin común".

8. Definición tradicional de Administración:

El proceso de planear, organizar, liderar, y controlar el trabajo de los miembros de la organización y de utilizar todos los recursos disponibles de la empresa para alcanzar objetivos organizacionales establecidos.

Planeación

Definiciones

- Proceso que permite la identificación de oportunidades de mejoramiento en la operación de la organización con base en la técnica, así como el establecimiento formal de planes o proyectos para el aprovechamiento integral de dichas oportunidades.
- Es la función que tiene por objetivo fijar el curso concreto de acción que ha de seguirse, estableciendo los principios que habrán de orientarlo, la secuencia de operaciones para realizarlo y las determinaciones de tiempo y números necesarios para su realización.
- "Hacer que ocurran cosas que de otro modo no habrían ocurrido". Esto equivale a trazar los planes para fijar dentro de ellos nuestra futura acción.
- Determinación racional de adónde queremos ir y cómo llegar allá.

La planeación implica que los administradores piensen a través de sus objetivos y acciones, y con anticipación, que sus acciones se basan en algún método, plan o lógica.

Organización

Es el proceso de disponer y destinar el trabajo, la autoridad y los recursos entre los miembros de una organización en una forma tal que puedan lograr los objetivos de la misma de manera eficiente.

Liderazgo

Implica dirigir, influir y motivar a los empleados para que realicen tareas fundamentales. Al establecer una atmósfera adecuada, se logra que los empleados den lo mejor de sí. Esta función también la podemos llamar "dirección", y ella cierra la brecha entre los planes, las estructuras organizacionales, las técnicas de control y la necesidad de que el personal entienda, esté motivado y contribuya a los objetivos del departamento y de la empresa.
La podemos definir también como el proceso de influir en las personas para contribuir a las metas de la organización.

Control

El administrador debe verificar que las acciones de los miembros de la organización la lleven a la obtención de sus metas.
Esto implica:

- Establecer normas de desempeño
- Medir el desempeño actual
- Comparar este desempeño con las normas establecidas
- Emprender acciones correctivas en caso necesario

En la práctica estas funciones no están separadas sino inter-relacionadas.

Evolución del concepto de administración

Teorías administrativas y sus enfoques

Teorías administrativas	**Principales enfoques**	**Enfasis**
Administración Científica	Racionalización del trabajo en el nivel operacional	En las tareas
Teoría Clásica	Organización Formal	En la estructura
Teoría Neoclásica	Principios generales de la administración, funciones del administrador, Organización formal	En la estructura
Teoría de la Burocracia	Burocrática, racionalidad organizacional	En la estructura
Teoría de las Relaciones Humanas	Organización formal e informal, motivación, liderazgo, comunicaciones y dinámica de grupos.	En las personas
Teoría del comportamiento organizacional	Estilos de administración, teoría de las decisiones, integración de los objetivos organizacionales e individuales.	En las personas
Teoría del desarrollo organizacional	Cambio organizacional planeado, enfoque de sistema abierto.	En las personas

Teoría estructuralista	Análisis intraorganizacional y análisis ambiental, enfoque de sistema abierto.	En el ambiente
Teoría de la contingencia	Administración de la tecnología	En la tecnología

Administración en la Antigüedad

A pesar de que la administración como disciplina es relativamente nueva, la historia del pensamiento administrativo es muy antigua, ya que nace con el hombre mismo, puesto que en todo tiempo ha habido necesidad de coordinar actividades, de tomar decisiones y de ejecutar, de ahí que en la administración antigua se encuentran muchos de los fundamentos administrativos de la actualidad y que pueden observarse en el código de Hammurabi, en el nuevo testamento, así como en la forma de conducir los asuntos en la antigua Grecia, Egipto, Roma y China, en donde se encuentran vestigios del proceso administrativo.

La eclesía era el organismo de mayor autoridad que existía en Grecia y formaban parte de ella todos los ciudadanos; las decisiones se tomaban por mayoría de votos y las mismas eran irrevocables.
En Grecia el emperador Pericles, 430 años antes de Cristo, dejó testimonio de la necesidad de una selección de personal adecuado e hizo un análisis sobre la democracia Griega.
En Egipto existía un sistema administrativo amplio con una economía planificada y un gobierno central de gran poder, basado en la fuerza y la compulsión. Aquí se creo el primer sistema de servicio civil.
El Sociólogo alemán Max Weber hizo un estudio sobre la administración antigua de Egipto, concluyendo, que se aplicaban procedimientos definidos y sistemáticos y se utilizaba un sistema administrativo burocrático.
En China el filósofo Confucio proporcionó una serie de reglas para la administración pública.
En Roma que vivió dos períodos, la República y el Imperio Romano, siendo en este último donde se produjeron transformaciones administrativas.
La administración del imperio Romano se caracterizó por la centralización.

China

A través de varios siglos, los chinos tuvieron un sistema administrativo de orden, con un servicio civil bien desarrollado y una apreciación bastante satisfactoria sobre muchos de los problemas modernos de administración pública.

Constitucion De Chow

Antes de gobernar organizar al mismo gobierno. Es imposible que alguien que no se organiza internamente o propiamente sea capaz de llevar la batuta de un estado.
Definición de funciones. El definir correctamente nos ahorra trabajo y se es más productivo.
Cooperación. Es indispensable para mostrar óptimos resultados.
Procesos eficientes. Si el proceso es bueno el resultado será mejor.
Formalidad de elementos humanos. Es la base de toda organización así que deben de esta bien

formalizados para un desempeño optimo y por consiguiente mejores resultados.
Personal optimo para Gobierno. En este renglón no se debe escatimar en personal pues le mejor capacitado es el que dará mejores secuelas.
Sanciones. Es la manera más lógica de y natural de corregir los errores.
Ajustes para valorar administración. Este nos servirá para saber como es que nos esta funcionando la administración llevada hasta ese momento.

Reglas De Confucio
1. Es obligación de los gobernantes estudiar un problema para dar así la mas adecuada resolución.
2. La solución a un problema deberá ser viéndolo desde una manera objetiva y sin rebasar las reglas de ética profesional.
Se trabaja hacia un pueblo, por lo cual el gobernante se debe tener un amplio criterio de resolución de problemas y de imparcialidad entre funcionarios.
La preocupación básica es lo económico, pero con esfuerzo colectivo se sobrepondrá.
La mente de un gobernante siempre debe de estar trabajando, para mejorar de alguna manera su gobierno sin preferencias de ningún tipo.
El administrador deberá ser de conducta intachable y sin egoísmos hacia sus colegas.

Egipto

En Egipto el tipo de administración se refleja una coordinación con un objetivo previamente fijado, su sistema el factor humano ya tenía cargos especiales es decir contaba con arquero, colectores de miel, marineros; algo importante de esta organización es que ya se contaba con un fondo de valores para los egipcios que se obtenía de los impuestos que el gobierno cobraba a sus habitantes, con el fin de después duplicarlo al comercializarlo por otros objetos.
Egipto tenía una economía planeada y, un sistema administrativo bastante amplio, que ha sido clasificado por Weber como "burocrático". Debido a los medios de comunicación marítimos fluviales, así como el uso comunal de la tierra, fue necesario que tales servicios y bienes fueran administrados de manera pública y colectiva, a través de el gran poder del gobierno central.
La idea que prevaleció en el antiguo Estado egipcio durante la IV, XI y XVIII dinastías fue que debía haber una severa coordinación de los esfuerzos económicos de toda población, a fin de garantizar a cada uno de los miembros de la comunidad, y para ella la misma como un todo, el más alto grado de prosperidad.
El sistema de los ptolomeos tuvo gran influencia en la administración de Filadelfia, puesto que en ella también la agricultura, el pastoreo, la industria y el comercio fueron conducidos dentro de iguales marcos de rigidez. Durante el Imperio Otomano (1520-1566 d. J.) se organizó una excelente administración de personal público, a pesar de que estaba concebida como un sistema de castas.
Tantas las formas burocráticas egipcias como sus seguidores levantinos tuvieron influencia en los criterios de gobierno e la región.

Roma

La organización de ROMA repercutió claramente en el éxito del imperio romano y aunque no quedan muchos documentos de su administración, se sabe que se manejaban por magisterios plenamente identificados en un orden jerárquico de importancia para el estado.

Después de varios siglos de monarquía, ejercida por soberanos etruscos, la república es instaurada en 509 a. J. C. En lo sucesivo, todos los ciudadanos forman el populus romanus, que se reúne en unas asambleas, los comicios. Cada año eligen unos magistrados encargados de gobernar el país: Cuestores (finanzas), ediles (administración), y pretones (justicia). En la cumbre, dos cónsules ostentan el poder ejecutivo, dirigen al ejército y realizan las funciones de jefes de estado. Acceder a estas diferentes funciones, una después de otra, constituye el curus honorum. Por ultimo, todos los antiguos magistrados componen el senado, que controla la política interior y dirige la política exterior.
Conquistadores atrevidos, cultivadores y comerciantes prudentes, los romanos manejan con igual ardor la espada que el arado. De esta manera engrandecen sus territorios e implantan una administración encargada de fomentar su desarrollo. Cada uno de los pueblos sometidos les suministra un importante contingente de soldados y esclavos. Los ciudadanos van abandonando progresivamente a estos últimos, cada día más numerosos, la mayor parte de sus tareas. Este sistema subsistirá durante varios siglos y permitirá que los romanos lleven a cabo una obra gigantesca y múltiple en los límites de su inmenso imperio: construcción de incontables monumentos, carreteras y acueductos; explotación de minas y canteras, irrigación. Pero también les quitará el sentido a la lucha y el esfuerzo, dejándolos finalmente desarmados ante las invasiones de los bárbaros, que acabarán con su poderío a partir del siglo IV de nuestra era.
El espíritu de orden administrativo que tuvo el Imperio Romano hizo que se lograra, a la par de las guerras y conquistas, la organización de las instituciones de manera satisfactoria. El estudio de estos aspectos se puede dividir en dos etapas principales por las cuales pasó la evolución romana, a saber; La República y el Imperio. Sin embargo, deben estudiarse también la monarquía y la autocracia militar. La primera época de la República comprendió a Roma como ciudad y la segunda a su transformación en Imperio mundial, y es justamente este último período el que puede ser de mayor interés de estudio por el ejemplo administrativo que ha dado. Cuando vino el Imperio, y éste extendió sus dominios, el sistema consular tuvo que transformarse en el proconsular que trató de lograr una prolongación de la autoridad del cónsul. Fue así como éstos y los pretores recibían una extensión del territorio bajo su tutela, después de un año de trabajo y pasaban así a tener jurisdicción sobre una provincia, bien como cónsules o como pretores.
Años más tarde, al comienzo de la Era Cristiana, vino otro cambio de gran importancia, al convertirse el imperio Romano en una autocracia militar establecida por Julio Cesar y mantenida luego por sus sucesores. Correspondió a Diocleciano (284-205 después de Jesucristo) reformar la autoridad imperial; eliminó los antiguos gobernadores de provincias y estableció un sistema administrativo con diferentes grados de autoridad. Fue así como debajo del emperador venían los prefectos pretorianos. Bajo ellos los vicarios o gobernantes de la diócesis, y subordinados a ellos los gobernadores de provincias hasta llegar finalmente a los funcionarios de menor importancia.
Entre las limitaciones mayores que se le apuntan a los sistemas administrativos romanos están la era de ampliación que tuvo la forma de gobierno de la ciudad de Roma al Imperio, y también la reunión de las labores ejecutivas con las judiciales, a pesar de que se reconoce que fueron aislados los conflictos de autoridad que se presentaron por equivocadas concepciones entre los derechos y los deberes particulares. Ello se subsanó por la disciplina que tuvieron en su organización jurídica, la cual ha servido de pilar fundamental a la concepción del derecho.

Grecia
La aportación que dio Grecia a la administración es grande y fue gracias a sus filósofos, algunos conceptos prevalecen aún.
SOCRATES. Utiliza en la organización aspectos administrativos, separando el conocimiento

técnico de la experiencia.
PLATON. Habla de las aptitudes naturales de los hombres, da origen a la especialización.
ARISTOTELES. Nos habla de que para lograr un estado perfecto.
PERICLES. Nos da unos de los principios básicos de la administración que se refiere a la selección de personal.
La administración gubernamental griega tuvo cuatro pasos evolutivos, puesto que sus estados tuvieron:

Monarquías
Aristocracias
Tiranías
Democracias

Con la única excepción de Esparta, en donde siempre hubo una aristocracia. La monarquía ateniense fue su primer sistema de gobierno y tuvo relativamente poca importancia desde un punto de vista administrativo; en tanto que el período aristocrático, que duró hasta el siglo y ante de Jesucristo, y el democrático si tuvieron una gran transcendencia. Mientras la democracia, el sistema de gobierno griego consistió en una asamblea popular denominada la eclesia, en el cual residía la autoridad máxima, y en ella participaban directamente todos los ciudadanos. Fue así ésa la primera manifestación que tuvo del concepto de gobierno de la mayoría y de que la soberanía del Estado la tiene el pueblo. En la eclesia se encuentran en buena parte las bases de nuestros sistemas democráticos actuales, con algunas limitaciones y diferencias. En la eclesia se discutían los asuntos y se formulaban las políticas a través de decisiones en las cuales tenían participación todos los ciudadanos.

La Administración en la Edad Media

Durante los últimos años del Imperio Romano el centralismo Administrativos se fue debilitando considerablemente y la autoridad real paso al terrateniente, alrededor del cual se agrupaban muchas personas, es decir, que en la Edad Media hubo una descentralización del gobierno, con lo que se diferenció de las formas administrativas que habían existidos anteriormente. Hubo una notable evolución de las ideas administrativas y se consolidaron instituciones como la Iglesia católica que tuvo mucho interés para los estudios de la administración, debido a su peculiar forma de organización y de funcionamiento.
En esta época la administración recibe un gran impulso cuando surgen en Italia, los fundamentos de la contabilidad moderna y las transacciones comerciales comienzan a racionalizarse cuando en 1340 Lucas Pacioli establece el método de contabilidad de la partida doble, Francisco Di Marco(1395) y Barbariego (1418), utilizan practicas de contabilidad denostó y los hermanos Soranzo (1410), hacen uso del libro diario y el mayor.

La administración en la Edad Moderna

A inicio de eta época surge en Prusia Austria un movimiento administrativo conocidos como cameralistas que alcanzó su mayor esplendor en 1560 y trató de mejorar los sistemas administrativos usados en esa época. Pusieron énfasis en el desarrollo de algunos principios administrativos, como fueron, el de selección y adiestramiento de personal, especialización de funciones y el establecimiento de controles administrativos.

En 1776 Adam Smith, considerado como el padre de la Economía clásica publica su obra "*La riquezas de las naciones"*, en donde aparece la doctrina del Laissez-Faire (dejar hacer, dejar pasar), que sirvió de base filosófica a la revolución industrial y que ha tenido su aplicación en la administración y en la economía; él anunció el principio de la división del trabajo, considerándolo necesario para especialización y para el aumento de la producción.

La administración en la Edad Contemporánea

Los historiadores están de acuerdo conque hubo una segunda revolución industrial de 1860 a 1914, llamada también revolución del acero y la electricidad, que sustituyó el hierro por acero como material básico para la industria en el campo de la energía.
La administración científica de Taylor surgida en esta época cumplió esa función, suministrándole las herramientas, técnicas necesarias para su expansión y desarrollo.

Teoría científica de Taylor

PRINCIPIOS ADMINISTRATIVOS
1.- Estudio de Tiempos y movimientos
2.- Selección de obreros
3.- Responsabilidad compartida
4.- Aplicación a la administración.

MECANISMOS ADMINISTRATIVOS
1. Estudio de tiempos y movimientos
2. Supervisión funcional
3. Sistemas o departamentos de producción
4. Principio de la excepción
5. Tarjetas de inscripción
6. Uso de la regla de calculo
7. Estandarización de las tarjetas de instrucción
8. Bonificación de las tarjetas de instrucción
9. Estudio de las rutas de producción
10.Sistema de clasificación de la producción
11.Costo de la producción.

CARACTERISTICAS DE LOS TRABAJOS HUMANOS
Descubre que no existe un sistema totalmente efectivo.
El puesto que desempeña el trabajador, no siempre va de acuerdo a sus capacidades.
Que no existen incentivos.
Que las decisiones se llevan a cabo en los niveles más altos.
Que la administración consta de principios aplicables a todas las empresas.

LIMITACIONES :
Sus aportaciones fueron muy importantes para la administración, pero también tuvo muchas críticas ; la federación del Trabajo Americana, lo consideraba un ser diabólico, debido a que los

trabajos de las personas bajo su sistema eran repetitivos y mecánicos, otra crítica muy grande fue la que recibió por abusar del término ciencia. Pero también hay que considerar que influye en sus estudios y resultados en Alemania, Inglaterra, Italia y en Estados Unidos, debido a que al llevar sus estudios cronometrados a las empresas, estas logran una alta productividad

Henry Fayol

Henry Fayol nace en Francia en el año de 1841 y muere en el año de 1925, entra a trabajar de gerente general a una compañía de minas de carbón que se encontraba en quiebra, después de 25 años era considerada una de las empresas más importantes a nivel mundial.

Aportaciones:

1.-Universalidad de la Administración: Demuestra que es una actividad común a todas las organizaciones: Hogar, empresa, gobierno, indicando que siempre que haya una organización cualquiera que sea su tipo debe de existir administración.

2.-Áreas funcionales: Para Fayol, deben de existir seis áreas funcionales dentro de la empresa:

1)Técnica: Se encarga de la producción
2)Comercial: Se encarga de la compraventa
3)Financiera: Se encarga del uso del capital
4)Contable: Se encarga de inventarios, balances y costos
5)Seguridad: Se encarga de proteger los bienes de la empresa y del empleado
6)Administrativa: Se encarga de utilizar adecuadamen5te los recursos.

3.- Modelo del proceso administrativo: Para Fayol, deben de existir dentro de la empresa ciertas etapas para poder desarrollar cualquier tipo de trabajo, dentro de ellas encontramos:

1) Previsión. (examinar el futuro)
2) Organización. (formular estructura)
3) Dirección. (Hacer funcionar los planes)
4) Coordinación. (Armonizar la información)
5) Control. (Verificar los resultados)

4.-Principios administrativos: Son catorce:

1.UNIDAD DE MANDO: Una sola persona debe de mandar a todos los subordinados.
2.AUTORIDAD: Toda empresa debe de tener una persona que los dirija.
3.UNIDAD DE DIRECCIÓN: Un programa para cada actividad.
4.CENTRALIZACIÓN: Todas las actividades deben ser manejadas por una sola persona.
NOTA: Actualmente encontramos que debido a las estructuras esto no resulta muy funcional para las empresas.
5.SOBORDINACIÓN DEL INTERÉS PARTICULAR AL GENERAL: Se debe buscar beneficiar a la mayoría.
6.DISCIPLINA: Se debe de lograr la disciplina para el buen funcionamiento de la empresa.
7.DIVISIÓN DEL TRABAJO: Se le debe de indicar a cada quien el trabajo que debe de realizar.
8.ORDEN : Cada cosa en su lugar y un lugar para cada cosa.
9.JERARQUÍA : Se debe de respetar la autoridad de cada nivel jerárquico.
10.JUSTA REMUNERACIÓN : Pago justo de acuerdo al trabajo realizado.
11.EQUIDAD : Los beneficios deben ser compartidos ; empresa-trabajadores.
12.ESTABILIDAD : El empleado debe de sentir seguridad en su trabajo.

13.INICIATIVA : Se debe de permitir al empleado que determine como deben de hacerse las cosas.
14.ESPIRITÚ DE GRUPO : Todos deben de colaborar entre sí.

5.- Perfil del administrador:
1) Cualidades físicas
2) Cualidades morales
3) Cualidades intelectuales
4) Conocimientos generales
5) Conocimientos específicos
6) Experiencia

6.-Importancia de la administración
Fayol determina que cualquier actividad que se desempeñe debe tener como base a la administración por lo que en sus estudios administrativos propone que deben de ser dados desde la primaria.

Limitaciones
Fayol fue un autor destacado de su época, sus aportaciones se reconocieron tiempo después y actualmente todas las empresas trabajan bajo ellas, por lo que no se puede concebir una empresa sin un proceso y una división de funciones o que no trabaje bajo los principios administrativos, etcétera.
Una de sus limitaciones fue que usó más la teoría que la práctica en sus trabajos.

Precursores de la Administración científica

La administración científica surgió durante la segunda revolución industrial, sus precursores más destacados son:

Charles Babbage
Es no sólo considerado como un precursor del pensamiento administrativo científico, sino también el de la computadora, ya que en 1822 fabrico una maquina mecánica de calcular que sirvió de orientación para la invención de las modernas computadoras.

Henry R. Towne
En 1886, ante la sociedad Norteamericana de Ingenieros Mecánicos, pronunció una conferencia titulada El Ingeniero como Economista, entre los asistentes se encontraba Frederick Taylor, en la misma se pedía que la administración se considerara como una ciencia. Ideó un plan de reparto de ganancias como sistema de pago de salario.

Henry Metacalfe
Se distinguió por implantar nuevas técnicas de control administrativos e ideó un buen sistema de control. Posteriormente Metacalfe fue considerado por Taylor como una persona muy eficiente. Publicó un libro titulado El Costo de Producción y la Administración de Talleres Públicos y Privados, considerado como una obra precursora de la administración científica.

Woodrow Wilson
Escribió un estudio sobre administración pública, es el más famoso y discutido articulo de la

ciencia de la administración que se haya jamás escrito en América. Wilson hizo una separación entre política y administración y le dio el calificativo de ciencia a la administración.

¿Cuál es la importancia de la administración?

Los mismos conceptos y propósitos analizados para la estructuración de una definición sobre la administración nos dan la pauta para determinar su importancia.
Las condiciones que imperan en esta época actual de crisis así como la necesidad de convivencia y labor de grupo, requieren de una eficiente aplicación de esta disciplina que se verá reflejada en la productividad y eficiencia de la institución o empresa que la requiera.

Para demostrar lo anterior se pueden tomar de base los siguientes hechos:

- La administración puede darse adonde exista un organismo social, y de acuerdo con su complejidad, ésta será más necesaria.
- Un organismo social depende, para su éxito de una buena administración, ya que sólo a través de ella, es como se hace buen uso de los recursos materiales, humanos, etc. con que ese organismo cuenta.
- En las grandes empresas es donde se manifiesta mayormente la función administrativa. Debido a su magnitud y complejidad, la administración técnica o científica es esencial, sin ella no podrían actuar.
- Para las pequeñas y medianas empresas, la administración también es importante, por que al mejorarla obtienen un mayor nivel de competitividad, ya que se coordinan mejor sus elementos: maquinaria, mano de obra, mercado, etc.
- La elevación de la productividad, en el campo económico social, es siempre fuente de preocupación, sin embargo, con una adecuada administración el panorama cambia, repercutiendo no solo en la empresa, sino en toda la sociedad.
- Para todos los países, mejorar la calidad de la administración es requisito indispensable, por que se necesita coordinar todos los elementos que intervienen en ésta para poder crear las bases esenciales del desarrollo como son: la capitalización, la calificación de sus trabajadores y empleados, etc.

¿Cuáles son las características de la administración?

Se ha indicado que la administración proporciona los principios básico mediante cuya aplicación es factible alcanzar éxito en el manejo de individuos organizados en un grupo formal que posee objetivos comunes.
Es necesario ahora agregar a tales conceptos las características de la administración y que son:

- **Universalidad**. El fenómeno administrativo se da donde quiera que existe un organismo social, porque siempre debe existir coordinación sistemática de medios. La administración se da por lo mismo en el Estado, en el ejército, en la empresa, en las instituciones educativas, en una comunidad religiosa, etc.

- **Su especificidad**. A pesar que la administración va siempre acompañada de otros fenómenos de distinta índole, el elemento administrativo es específico y distinto a los que acompaña. Se puede ser un magnífico ingeniero de producción y un pésimo administrador.
- **Su unidad tempora**l. Aunque se diferencien etapas, fases y elementos del fenómeno administrativo, éste es único y, por lo mismo, en todo instante de la operación de una organización se están dando, en mayor o menor proporción, todos o la mayor parte de los elementos administrativos. Así, al hacer los planes, no por eso se deja de mandar, de controlar, de organizar, etc. Por lo mismo, se puede afirmar que es un proceso interactivo y dinámico.
- **Su unidad jerárquica**. Todos los poseen carácter de jefes en un organismo social, participan en diversos grados y modalidades, de la misma administración. Así, en una organización forman un solo cuerpo administrativo, desde el Presidente, hasta el último supervisor.

Administración y las personas

Estilos de liderazgo

- Líder orientado a la tarea
  - Autocrático
  - Restrictivo
  - Directivo
  - Socialmente distante
- Líder orientado a las personas
  - Democrático
  - Tolerante
  - Participativo
  - Comprensivo

Funciones del trabajo directivo

- Informacionales: supervisa, difunde, es portavoz
- Decisionales: emprendedor, soluciona de problemas, asigna recursos, negocia
- Interpersonales: representante, enlace, líder

La función de dirección implica armonizar objetivos, necesidades de los individuos y demandas de la empresa.

Definición de Organización

Dos o más personas que trabajan juntas en forma estructurada para alcanzar un objetivo específico o un conjunto de objetivos.

Organización formal e informal

Organización formal

Es la organización basada en una división del trabajo racional, en la diferenciación e integración de los participantes de acuerdo con algún criterio establecido por aquellos que manejan el proceso decisorio. Es la organización planeada; la que está en el papel.
Es generalmente aprobada por la dirección y comunicada a todos a través de manuales de organización, de descripción de cargos, de organigramas, de reglas y procedimientos, etc.
En otros términos, es la organización formalmente oficializada.

Organización informal

Es la organización que emerge espontánea y naturalmente entre las personas que ocupan posiciones en la organización formal y a partir de las relaciones que establecen entre sí como ocupantes de cargos.
Se forma a partir de las relaciones de amistad o de antagonismo o del surgimiento de grupos informales que no aparecen en el organigrama, o en cualquier otro documento formal.
La organización informal se constituye de interacciones y relaciones sociales entre las personas situadas en ciertas posiciones de la organización formal.
Surge a partir de las relaciones e interacciones impuestas por la organización formal para el desempeño de los cargos.
La organización informal comprende todos aquellos aspectos del sistema que no han sido planeados, pero que surgen espontáneamente en las actividades de los participantes, por tanto, para funciones innovadoras no previstas por la organización formal.

Desempeño Administrativo

La medición de qué tan efectivo y eficiente es un administrador, qué tan bien determina o logra objetivos convenientes.

- *Eficiencia*: hacer correctamente las cosas, es decir, minimizar el costo de los recursos conque se obtienen las metas.
- *Eficacia*: hacer las cosas correctas, es decir, capacidad de escoger los objetivos adecuados

Administración y Sistemas de Información

Introducción

El papel de las computadoras en las organizaciones

Se estima que hoy en día más del 50% de los administradores utilizan las computadoras a diario, para las siguientes funciones:

- Facilitar la obtención, manejo y comunicación de la información a lo largo de la línea jerárquica, así como también entre los trabajadores del mismo nivel.
- Automatizar las operaciones
- Apoyar la planeación y la toma de decisión
- Simplificar el control administrativo

¿Cuándo es especialmente útil el uso de computadoras?

- Gran volumen de datos de rutina a ser procesados
- Actividades y funciones repetitivas
- Cuando es necesario almacenar y tener acceso rápido a gran volumen de datos y de información
- Cuando es esencial el procesamiento rápido y los registros de negocio de última hora
- Cuando es necesario realizar cálculos complejos

Componentes de los sistemas de información

- Hardware
- Software
- Datos
- Gente: especialistas técnicos y usuarios finales
- Procedimientos: normas y políticas preestablecidas que rigen la operación del sistema de computación y la forma en que los usuarios finales interactúan con el sistema.

Objetivo de un Centro de Cómputo

Prestar servicios a diferentes áreas de una organización ya sea dentro de la misma empresa, o bien fuera de ella, tales como: producción, control de operaciones, captura de datos, programación, dibujo, biblioteca, etc.
Los diversos servicios que puede prestar un centro de computo, pueden dividirse en departamentos a áreas específicas de trabajo.

Niveles de Planeación

La planeación considerada como uno de los principales elementos del proceso administrativo, es de fundamental importancia dentro de la estructuración de un Centro de Cómputo; como tal considera los siguientes niveles:

- Planeación Estratégica.
- Planeación de Recursos.
- Planeación Operativa.
- Planeación de Personal.
- Planeación de Instalaciones Físicas.

En realidad estos niveles responden a las siguientes interrogantes básicas, ¿Que?, ¿Quien?, ¿Dónde?, ¿Cuándo? ¿Cómo? y ¿Por qué?.

- *Planeación Estratégica*. Se refiere a las estrategias a seguir en la construcción del Centro de Cómputo. ¿Por qué construirlo?. Cuando se responde a este cuestionamiento, pueden inferirse los caminos a seguir para la construcción del mismo.
- *Planeación de Recursos*. Dentro de este ámbito deben considerarse los recursos económicos que va a requerir la construcción del Centro de Cómputo. ¿Cuánto dinero se va a ocupar?.
- *Planeación Operativa.* ¿Cómo va a funcionar el Centro de Cómputo?, ¿Qué Software será necesario?, ¿Qué Hardware se requerirá?, ¿Qué servicios va a prestar?, etc.
- *Planeación de Personal*. ¿Quiénes van a operar al Centro de Cómputo?, ¿Cuáles serán sus funciones?, ¿Qué cantidad de personal será necesaria?, etc.
- *Planeación de Instalaciones Físicas*. ¿En dónde estará ubicado en Centro de Cómputo?, ¿Cuántas secciones será necesario construir?,¿En dónde serán ubicados los servidores o la macrocomputadora?, ¿Qu condiciones de ventilación serán necesarias?, etc.

Planeación de recursos

La planeación de recursos en para un centro de cómputo es aquella que establece los objetivos y determina un curso de acción a seguir, de los siguientes elementos:

- Instalaciones: Edificios y acondicionamiento del mismo, plantas de emergencia, dispositivos de seguridad, etc.
- Equipo: Equipo de cómputo necesario para su funcionamiento, periféricos, etc.
- Materiales de producción: Materias primas para su funcionamiento, así como materiales directos e indirectos.

Planeación operativa

La planeación operativa de un centro de cómputo consiste en realizar un detallado análisis de necesidades de la empresa y definir en base a estas necesidades una plataforma tecnológica con una infraestructura en hardware, software, personal operativo, etc. que soporte las operaciones de la empresa y se utilice como el medio de procesamiento de información.

Planeación de instalación física y ubicación física

La ubicación física e instalación de un Centro de Cómputo en una empresa depende de muchos factores, entre los que podemos citar: el tamaño de la empresa, el servicio que se pretende

obtener, las disponibilidades de espacio físico existente o proyectado, etc.
Generalmente, la instalación física de un Centro de Cómputo exige tener en cuenta por lo menos los siguientes puntos:

- Local físico. Donde se analizará el espacio disponible, el acceso de equipos y personal, instalaciones de suministro eléctrico, acondicionamiento térmico y elementos de seguridad disponibles.
- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- Seguridad física del local. Se estudiará el sistema contra incendios, teniendo en cuenta que los materiales sean incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.). También se estudiará la protección contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
- Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

Organización de un Centro de Cómputos

Forma de operar un centro de cómputo

Un Centro de Procesamiento de Datos (CPD) o Centro de cómputo, es el conjunto de recursos físico, lógicos, y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa.
Las principales funciones que se requieren para operar un centro de cómputo son las siguientes:

- Operar el sistema de computación central y mantener el sistema disponible para los usuarios.
- Ejecutar los procesos asignados conforme a los programas de producción y calendarios preestablecidos, dejando el registro correspondiente en las solicitudes de proceso.
- Revisar los resultados de los procesos e incorporar acciones correctivas conforme a instrucciones de su superior inmediato.
- Realizar las copias de respaldo (back-up) de la información y procesos de cómputo que se realizan en la Dirección, conforme a parámetros preestablecidos.
- Marcar y/o señalizar los productos de los procesos ejecutados.
- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- Velar porque el sistema computarizado se mantenga funcionando apropiadamente y estar

vigilante para detectar y corregir fallas en el mismo.
- Realizar labores de mantenimiento y limpieza de los equipos del centro de cómputo.
- Aplicar en forma estricta las normas de seguridad y control establecidas.
- Mantener informado al jefe inmediato sobre el funcionamiento del centro de cómputo.
- Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección para el desarrollo de las funciones asignadas.

Principales áreas de un Centro de Cómputo

Dentro de una empresa, el Centro de proceso de Datos ó Centro de Cómputos cumple diversas funciones que justifican los puestos de trabajo establecidos que existen en él, las cuales se engloban a través de los siguientes departamentos:

- *Explotación de sistemas o aplicaciones*. La explotación u operación de un sistema informático o aplicación informática consiste en la utilización y aprovechamiento del sistema desarrollado. Consta de previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema, supervisión de trabajos, etc.
- *Soporte técnico a usuarios*. El soporte, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar, instalar y mantener el sistema operativo adecuado, del diseño y control de la estructura de la base de datos, la gestión de los equipos de teleproceso, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.
- *Gestión y administración del propio Centro de Procesamiento de Datos*. Las funciones de gestión y administración de un Centro de Procesamiento de Datos engloban operaciones de supervisión, planificación y control de proyectos, seguridad y control de proyectos, seguridad general de las instalaciones y equipos, gestión financiera y gestión de los propios recursos humanos.

Operación

Esta área se encarga de brindar los servicios requeridos para el proceso de datos, como son el preparar los datos y suministros necesarios para la sala de cómputo, manejar los equipos periféricos y vigilar que los elementos del sistema funcionen adecuadamente.
En esencia el personal del área operativa se encarga de alimentar datos a la computadora, operar el "hardware" necesario y obtener la información resultante del proceso de datos.

Operadores

- Los operadores de computadoras preparan y limpian todo el equipo que se utiliza en el proceso de datos, mantienen y vigilan las bitácoras e informes de la computadora, montan y desmontan discos y cintas durante los procesos y colocan las formas continuas para la impresión.
- También documentan las actividades diarias, los suministros empleados y cualquier condición anormal que se presente.
- El papel de los operadores es muy importante debido a la gran responsabilidad de operar la unidad central de proceso y el equipo periférico asociado en el centro de cómputo.
- Un operador de computadoras requiere de conocimientos técnicos para los que existen programas de dos años de capacitación teórica, pero la práctica y la experiencia es generalmente lo que necesita para ocupar el puesto.

Area de Producción y Control

Tanto la Producción como el Control de Calidad de la misma, son parte de las funciones de este Departamento.

Funciones

- Construir soluciones integrales (aplicaciones) a las necesidades de información de los usuarios.
- Usar las técnicas de construcción de sistemas de información orientadas netamente a la productividad del personal y a la satisfacción plena del usuario.
- Construir equipos de trabajo con la participación del usuario y del personal técnico de acuerdo a metodologías establecidas.
- Mantener comunicados a los usuarios y a sus colaboradores de los avances, atrasos y problemas que se presentan rutinariamente y cuando sea necesario a través de medios establecidos formalmente, como el uso de correo electrónico, mensajes relámpagos o flash.
- Mantener programas de capacitación para el personal técnico y usuarios.

Area de Análisis de Sistemas

Los analistas tienen la función de establecer un flujo de información eficiente a través de toda la organización.
Los proyectos asignados a los analistas no necesariamente requieren de la computadora, mas bien necesitan el tiempo suficiente para realizar el estudio y la proposición de soluciones de los problemas, planteando diferentes alternativas.
La realización de cualquiera de las soluciones puede durar varias semanas o meses dependiendo de la complejidad del problema.
Los proyectos típicos de sistemas pueden implicar el diseño de reportes, la evaluación de los trabajos efectuados por el personal de los departamentos usuarios, la supervisión de cambios de equipo la preparación de presupuesto en el área de cómputo.
Los analistas pueden ser egresados de diferentes carreras y básicamente los requisitos para estos son: educación profesional formal y experiencia practica, esta última solo se logra después de haber trabajado en el área de programación.
Existen diferentes títulos de analistas: Analista Junior, Aprendiz de Sistemas y Analista Senior que indican diferentes grados de experiencia, entrenamiento y educación. A su vez estos pueden tener todavía más clasificaciones dependiendo del tamaño de la organización, o bien puede haber analistas programadores que realizan tanto la función de analistas como la de programadores, esto indica una doble responsabilidad. Además los analistas pueden estar agrupados en equipos cuyas funciones son coordinadas por analistas líder o jefes de análisis.

Area de Programación
Los programadores toman las especificaciones de los sistemas realizados por los analistas y las transforman en programas eficientes y bien documentados para las computadoras.

Departamento o área de Implementación
Esta área es la encargada de implantar nuevas aplicaciones garantizando tanto su calidad como su adecuación a las necesidades de los usuarios.
Algunas funciones principales generales que realiza esta área son:

- Coordinar con las áreas de sistemas y usuarios la implantación de las aplicaciones.

- Diseñar los planes de calidad de las aplicaciones y garantizar su cumplimiento.
- Validar los nuevos procedimientos y políticas a seguir por las implementaciones de los proyectos liberados.
- Probar los productos y servicios a implementar antes de ser liberados al usuario final.
- Elaborar conjuntamente con el área de Programación o Desarrollo, los planes de capacitación de los nuevos usuarios.
- Coordinar la presentación de las nuevas aplicaciones a los usuarios.
- Supervisar el cumplimiento de los sistemas con la normatividad establecida.

Area de Soporte Técnico
Área responsable de la gestión del hardware y del software dentro de las instalaciones del Centro de Cómputo, entendiendo por gestión: estrategia, planificación, instalación y mantenimiento. Algunas funciones principales generales que realiza esta área son:

- Planificar la modificación e instalación de nuevo software y hardware.
- Evaluar los nuevos paquetes de software y nuevos productos de hardware.
- Dar el soporte técnico necesario para el desarrollo de nuevos proyectos, evaluando el impacto de los nuevos proyectos en el sistema instalado.
- Asegurar la disponibilidad del sistema, y la coordinación necesaria para la resolución de los problemas técnicos en su área.
- Realizar la coordinación con los técnicos del proveedor con el fin de resolver los problemas técnicos y garantizar la instalación de los productos.
- Proponer las notas técnicas y recomendaciones para el uso óptimo de los sistemas instalados.
- Participar en el diseño de la Arquitectura de Sistemas.

Evolución histórica de los Sistemas de Información

Sistemas de proceso transaccional (TPS)

- Aparecieron en 1960s
- Funciones: alta rutina, bien entendibles, decisiones repetitivas, intensivos en entrada/salida de información
- Ejemplo: manejo de personal, contabilidad central
- Tecnología: mainframes, tarjetas perforadas, ingreso batch
- Objetivos: hacer que trabaje el sistema de la computadora central
- Posibles problemas: altos costos de mantenimiento, duplicación de datos, insatisfacción de los usuarios

Sistema de información administrativa (MIS)

- Aparecieron en 1970s
- Funciones: menos estructurados, resolución de problemas generales
- Ejemplo: reportes de alto nivel en grandes bases de datos
- Tecnología: minis, con acceso en lína, lenguajes de programación de alto nivel, sistemas de

tiempo real, transacciones únicas, bases de datos centralizadas, integración de sistemas
- Fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.
- Objetivos: integración de sistemas, compartir datos, observar tendencias
- Problemas: altos costos de desarrollo de software, y de entrenamiento de personal, necesidad de estándares

Sistema de soporte de decisiones (DDS)

- Aparecieron en 1980s y 1990s
- Funciones: soporta decisiones de políticas en un paso ("one shot")
- Ejemplo: administración de portafolio de inversiones, sistemas de soporte a pilotos aéreos
- Tecnología: minis, estaciones de trabajo, acceso a PC, comunicaciones remotas, bases de datos distribuidas, procesamiento integrado (voz, datos, videos), procesamiento distribuido
- Objetivos: reportes rápidos y significativos para ofrecer soporte a los tomadores de decisión
- Problemas: manejo de bases de datos distribuidas en tiempo real, altos costos de desarrollo para crear el sistema, requerimiento frecuente de entrenamiento a personal ejecutivo

En conclusión, el sistema de apoyo para decisiones es un sistema interactivo de computadora, de fácil acceso y operación, a menos de personas que no son especialistas en computadoras y que usan el DSS para que les ayude a planificar y tomar decisiones. El uso del DSS está extendiéndose, conforme a los avances recientes en máquinas y programas de computadoras, permiten que los gerentes y otros empleados designados tengan acceso basándose en datos de MIS.
El uso generalizado de la micro computadoras ha permitido a los gerentes crear sus propias bases de datos y manejar información, en forma electrónica, conforme a la necesidad, en lugar de tener que esperar los informes emitidos por el departamento de EDP/MIS.

Sistema de información estratégicos (SIS)

- Uso innovador de viejas y nuevas tecnologías
- Diferencias con otros sistemas:
  - cambian la forma en que compiten las empresas
  - tienen un enfoque externo (hacia fuera)
  - están asociados a riesgos mayores de proyecto
  - son innovadores y por lo tanto, difíciles de copiar

Este tipo de sistemas es deseable porque puede usarse para generar una ventaja competitiva. Ventaja competitiva significa que una firma puede proporcionar ***más valor*** a sus clientes y el mismo precio que sus rivales, o puede proveer ***el mismo valor*** a sus clientes pero a ***menor*** precio que sus rivales.

Por último, es importante aclarar que algunos autores consideran un cuarto tipo de sistemas de información denominado Sistemas Personales de Información, el cual está enfocado a incrementar la productividad de sus usuarios.

Sistema de información administrativa (MIS)

Definición

Es un sistema de información basado en la computadora para planear, tomar decisiones y controlar de manera más eficaz.

Otra definición

Método formal de poner a disposición de los administradores la información confiable y oportuna que se necesita para facilitar el proceso de la toma de decisiones y permitir que las funciones de planeación, control y operaciones se realicen eficazmente en la organización.

Cada vez más la información está siendo vista como un factor clave para ayudar a los administradores a comprender el complejo medio externo. Por lo tanto la información es vista como un activo invaluable, que necesita ser manejado cuidadosamente y protegido.

Naturaleza de la información

- Datos: números y hechos en bruto, sin analizar
- Información: datos que han sido organizados o analizados de alguna manera significativa.

Factores para la evaluación de la información

- Calidad: cuanto más exacta, los administradores podrán recurrir a ella con más confianza en el momento de tomar una decisión. No obstante, el costo de la información aumenta cuanto más exacta es.
- Oportunidad de la información: disponible en el momento indicado para la persona apropiada.
- Cantidad: debe ser suficiente, pero evitando datos irrelevantes o inútiles.
- Relevancia: debe estar relacionada con las actividades y responsabilidades del administrador.

Diseño de un sistema de información administrativa

Etapas:

1. Estudio y definición del problema
2. Diseño conceptual
3. Diseño detallado
4. Implantación

Lineamientos para un diseño efectivo

- Hacer que los usuarios formen parte del equipo de diseño
- Estudiar el costo monetario y de tiempo del sistema
- Considerar las alternativas para el desarrollo de software de la organización
- Anteponer la relevancia y selectividad antes que la simple cantidad: un administrador necesita "suficiente" información para tomar una decisión bien fundada, pero el exceso de información puede abrumarlo. El sistema de información administrativa *filtra* la información de modo que sólo la más relevante sea proporcionada al administrador que la necesite. Además, un buen sistema de información *condensa* de modo que lo más importante pueda captarse con rapidez.
- Realizar pruebas preliminares del sistema antes de instalarlo:
    - instalación directa: reemplazo total del sistema antiguo
    - instalación paralela
    - instalación de prueba
    - instalación por fases
- Capacitar con sumo cuidado y documentación escrita a los operadores y usuarios del sistema.

Problemas en la implantación de un sistema de información administrativa

Resistencia organizacional (G.W.Dickson, J.K.Simmons): se deben tener en cuenta los siguientes aspectos:

- ¿El MIS rompe con los límites departamentales establecidos? Por ejemplo, puede que para hacer mejor uso del sistema, dos departamentos se fusionen (compras e inventarios), y la gente verse obligada a modificar la forma en que trabajan.
- ¿El MIS rompe con el sistema informal? Puede alterarse la red de comunicaciones informales a medida que avanza la implantación del sistema
- ¿El MIS exige características individuales específicas? Las personas con mucha antigüedad en la empresa conocen bien su trabajo y saben cómo hacer que las cosas funcionen con el sistema actual. Pueden ofrecer resistencia al cambio.
- ¿El MIS está apoyado por la cultura organizacional? Si la alta dirección está alejada de los empleados, o si la cultura organizacional apoya un comportamiento inflexible, tiende a dificultarse la implantación del sistema.
- ¿Los empleados tienen una opinión en cuanto a la manera en que se ha implementado el cambio? En general, cuando los administradores y subordinados toman juntos las decisiones, hay mayores chances de éxito.

Formas de rechazo a la implantación de un nuevo sistema

- Agresión: puede llegar al sabotaje (uso incorrecto del equipo, introducción de información incompleta o inadecuada, destrucción de hardware o software)
- Proyección: mecanismo psicológico que consiste en atribuirle los problemas a alguien o

alguna cosa. Ocurre cuando los administradores atribuyen al sistema los problemas causados por error humano o por factores ajenos a él.
- Prevención: los individuos se defienden alejándose de una situación frustrante o evadiéndola. Los administradores actúan de esta manera cuando ignoran los resultados producidos por el sistema y recurren a sus propias fuentes.

Grupos de trabajo y posibles comportamientos

Subgrupo organizacional	**Relación con el MIS**	**Comportamiento disfuncional**
Alta dirección	Generalmente ajena a los sistemas	Previsión
Personal técnico	Cambio de los diseñadores y agente de los sistemas	Ninguna
Administración operativa	Controlada desde arriba por sistemas; los nuevos sistemas modifican el contenido el trabajo y el contexto	Agresión, rechazo y proyección
Personal operativo	Muy poco afectado; se eliminan puestos, cambian patrones de los puestos	Proyección
No administrativo	Ofrece insumos a los sistemas	Agresión

Superación de los problemas de implantación

- Orientación a los usuarios: debe satisfacer plenamente las necesidades de los usuarios con un mínimo de ajuste y nuevo aprendizaje.
- Participación: muchos problemas pueden superarse si los futuros usuarios se integran al equipo de preparación del sistema.
- Comunicación: los objetivos y características del sistema deben comunicarse con claridad a todos los miembros del equipo del MIS y a los usuarios.
- Redefinición de las medidas de desempeños: un sistema que requiere nuevos procedimientos y criterios valorativos debe acompañarse de incentivos para estimular un buen desempeño y la aceptación del sistema.
- Nuevos retos: un MIS puede liberar a muchos administradores de mandos medios de muchas actividades rutinarias y aburridas. También les brinda la posibilidad de utilizar la información que les brinda de una forma más creativa y productiva.

Sistemas de soporte de decisiones (DSS)

Definición

Es un sistema interactivo, de fácil acceso y operado por personas no especializadas en computación, para ayudarse en la planeación y en las funciones de la toma de decisiones.

Diferencias entre MIS y DSS

- Está diseñado para manejar la información, y no esencialmente almacenarla y recuperarla, como muchos MIS
- Operado directamente por los usuarios
- Ayuda a los administradores a adoptar decisiones no rutinarias

Areas de la Administración de Sistemas de Información altamente disponibles

Hoy en día abundan los sistemas que deben estar siempre disponibles. Para que un sistema esté siempre disponible se necesita vigilancia constante. Las herramientas, equipos de trabajo y procesos involucrados en el mantenimiento del sistema están integrados a esta función. Tener las mejores herramientas no significa nada si el personal involucrado con el sistema no está entrenado y comprometido en un rol activo a mantener la disponibilidad.
Las siguientes son áreas de administración que cubren diferentes aspectos de la Administración de Sistemas:

- *Administración de la capacidad*
- *Administración/Manejo de problemas*
- *Administración del cambio*
- *Administración del nivel de servicio*
- *Seguridad*
- *Administración de la disponibilidad*

Para administrar un sistema de alta disponibilidad requiere una mezcla interrelaccionada de hardware, software, gente, procesos, y estándares. La importancia de los estándares creció con el advenimiento de la tecnología distribuida. Esta introdujo un alto riesgo de falla debido a la cantidad de interdependencias de hardware y software dispares, que necesitan comunicarse entre ellos. El sistema altamente disponible ha crecido más allá de la simple transferencia de datos introduciendo videos, voz, y datos que interactúan entre ellos y con sistemas fuera de nuestro universo personal.

Administración de la Capacidad

Definición

Es el proceso de monitorear, analizar y planificar el uso efectivo de los recursos computacionales.

El manejo de la capacidad se ha vuelto complejo. Toma el esfuerzo combinado de personal

entrenado y visionario, procesos diseñados para cambiar, y herramientas específicas para el tipo de medición necesario.
En el pasado era posible incrementar la capacidad simplemente comprando un disco más grande, más RAM o un módem más rápido. Hoy, debe monitorearse el ancho de banda; y la capacidad y los patrones de flujo de los datos a través del hardware deben ser medidos. Deben observarse las interacciones de las aplicaciones, y además esta interacción con el hardware. Todo esto mientras se trata de predecir el futuro.
Objetivos generales

- Contribuir a la planeación estratégica del negocio
- Detectar precozmente problemas de TI, y planificar la solución
- Mejorar la comunicación entre el personal de TI y la dirección y personal no especializado.
- Promover la responsabilidad por el uso de los sistemas de TI.
- Proporcionar cifras medibles de desempeño de TI, como base para la planeación estratégica de TI.

Esto hace evidente la necesidad de contar con una *política* y *procedimientos* claros sobre la Administración de Capacidad, así como la integración con los procesos del negocio.

Objetivos para sistemas altamente disponibles

El plan de capacidad usado para ayudar a construir sistemas altamente disponibles tiene varios objetivos:

- Afinar sistemas y redes existentes
- Dimensionar nuevos sistemas y redes
- Predecir crecimiento y actualización de sistemas existentes y redes
- Predecir analisis para anticipar excepciones de capacidad
- Analizar tendencias de sistemas existentes y redes.

Estos objetivos junto con los procesos y la gente encargada del manejo de la capacidad ayudarán a elegir las herramientas necesarias para monitorear, medir el desempeño, y reunir información sobre la capacidad.

Fases

Los procesos básicos necesarios para monitorear, medir, y planear la capacidad son:

1. *Decidir qué es lo que se va a medir en términos de capacidad.*

   Implica identificar la composición de la carga de trabajo (caracterización de la carga de trabajo).
   Esta es la definición de qué datos, quién está haciendo el trabajo, y cuándo. Esta información se reúne entrevistando usuarios y agrupando los tipos de datos de acuerdo a lo que se quiere medir. La medición de las aplicaciones puede agruparse según quién está haciendo el trabajo, mientras que el monitoreo de los picos de flujo de datos puede agruparse según qué clase de datos se está moviendo de un lado a otro.

2. *Recolectar datos*

   Estos datos históricos serán usados para predecir el volumen de la carga de trabajo anticipadamente, en diferentes puntos del tiempo futuro.
   ¿Qué se va a medir?
   - espacio libre en disco y uso del disco
   - uso de memoria y CPU
   - cantidad de usuarios
   - tiempos de ejecución
   - disponibilidad de recursos
   - ancho de banda de la red
   - configuración de servidores

Si se trata de clientes internos, esta información debería ser distribuida a todos los interesados para que den sus aportes y estén informados sobre el uso que dan a los recursos informáticos.

3. *Monitorear desempeño*

   Debe compararse la información con estadísticas de manejo de recursos, o convenios de nivel de servicio, o con los procesos del negocio. Luego debe analizarse para detectar posibles problemas, teniendo en cuenta cambios operados en los procesos, o previstos para el futuro.

4. *Generar planes de capacidad*

   Crear escenarios "What-if", y análisis de tendencias
   Deben proponerse soluciones a los problemas detectados o cambios surgidos en el manejo del negocio, y con ellas, definir un plan de acción que se comunicará al personal encargado de implementarlas. Además, hay que incluir los cambios necesarios en el monitoreo.

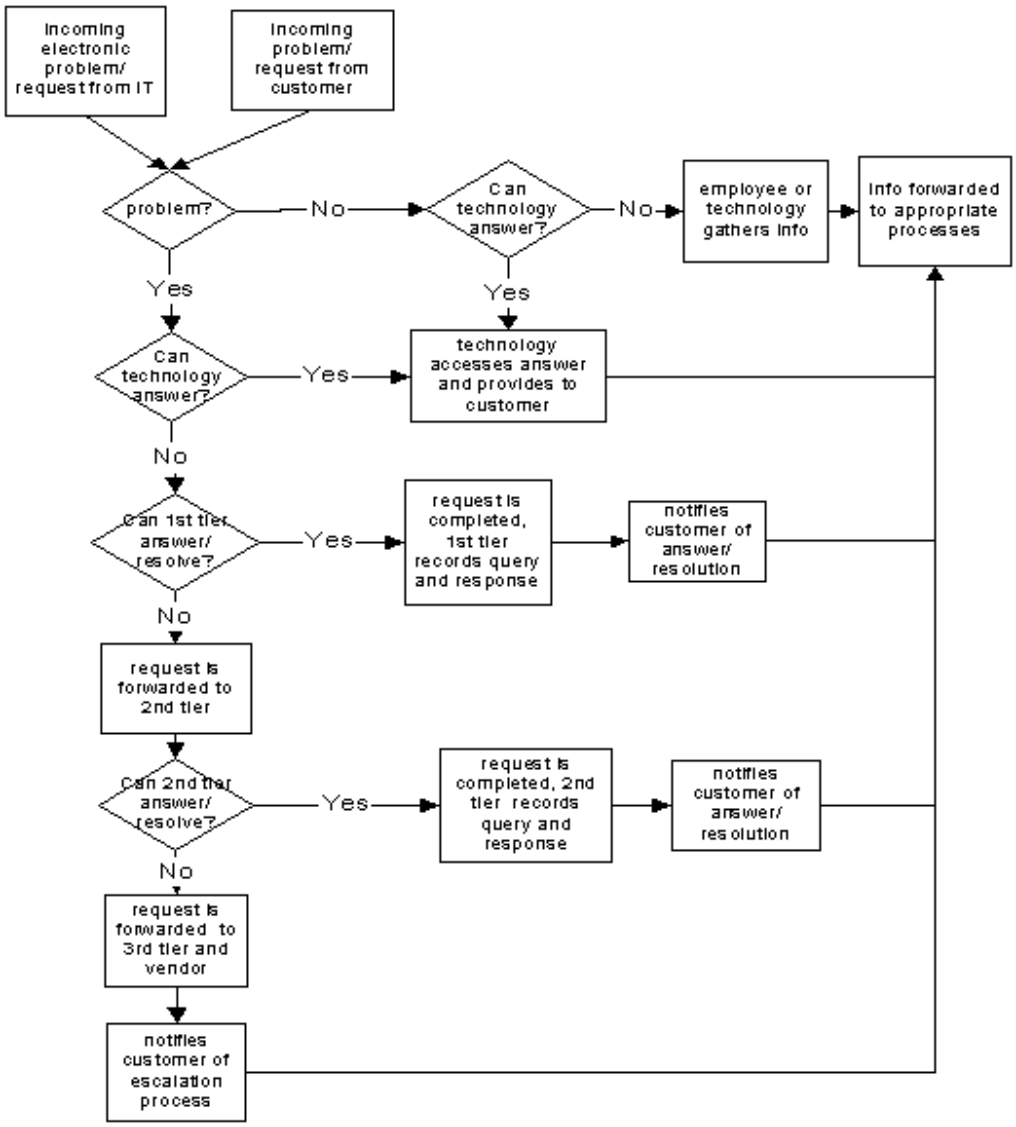
Factores

- *Infraestructura de TI*: hardware, software
- *Información sobre el negocio*: contratos, directivas estratégicas, nuevos requerimientos del negocio.
- *Personal*: personal que administra los datos, o que mantiene aplicaciones, o propietarios de sistemas de aplicación. Todas estas personas deben estar involucradas en el proceso, y conocer los procedimientos de la Administración de Capacidad, y qué rol tienen en ellos.

Manejo de Problemas

El manejo de problemas en su forma más básica es la persona, proceso, y tecnología que resuelve un problema de un cliente. El manejo de problemas ya no reside sólo en help desk. Hoy en día, llevar la pista, alertar, escalar, y resolver problemas están incluidos en una mezcla compleja de servicios administrados en el Service Desk (antes conocido como help desk).
Contestar una pregunta o resolver un problema que presentó un cliente requiere integración de procesos que asegure que el primer contacto con el cliente lo satisface. Un proceso simple puede

verse como:



Administración del cambio

La administración del cambio es una de las preocupaciones mayores de la mayoría de los gerentes de IT. Esto se debe a la creciente complejidad de la computación necesaria para llevar adelante el negocio, interna y externamente. Los sistemas complejos que deben funcionar juntos requieren un manejo inteligente.
Los precursores fundamentales de la administración del cambio son los estándares y políticas. La proliferación de las alternativas de hardware y software obligan a tener una visión clara de los servicios designados como altamente disponibles.
Deberían crearse grupos de trabajo que incluyan:

- Clientes
- Desarrolladores

- Proveedores de servicio de IT
- Quienes resuelven los problemas
- Otros afectados por los cambios

Administración del nivel de servicio

Esto se lleva a cabo con lo que se llama "Service Level Agreement" (SLA). Esto consiste en un acuerdo operacional entre la organización IT, y sus clientes y socios de negocios. SLAs definen características y parámetros y procedimientos de soporte asociados para un servicio ofrecido por IT al cliente del negocio.
Los servicios se comparan con un conjunto de objetivos (disponibilidad, confiabilidad, cambio, utilidad, capacidad, seguridad) donde cada objetivo define un conjunto de atributos medibles. Los tipos de objetivos son:

- Condición de Operación – disponibilidad, confiabilidad, capacidad, seguridad
- Flujo de trabajo de procesos – utilidad, cambio
- Encuesta de satisfacción del cliente

Los SLA generalmente contienen:

- Definición de servicios, que incluye un manifiesto o cadena de hardware y software
- Especificación de horas y días de servicios que serán ofrecidos
- Explicación de procedimiento de reporte de problemas – tiempos esperados y contactos para realizar cambios
- Especificación de la meta de nivel de servicio para la operación (calidad), incluyendo:
    - Disponibilidad y confiabilidad promedio para el período de servicio
    - Tiempo de respuesta y entrega promedio y menor

Un Service Level Agreement (SLA) es un papel que vale la pena en tanto la gente, procesos y tecnología necesarios para medir, monitorear y reportar estén disponibles.
SLA es una buena herramienta para especificar servicios y su nivel de desempeño, pero es importante notar que debe existir un fundamento de tecnología y administración de sistemas planeado antes de entrar en tal acuerdo.

Administración de la disponibilidad

La administración de la disponibilidad es el seguimiento para detectar incidentes en los servidores, red, aplicaciones y bases de datos que hacen funcionar el negocio. Hay tres áreas de interés:

- Mantenibilidad
- Confiabilidad
- y practicidad o utilidad.

Mantenibilidad

Mantenibilidad incluye la habilidad de controlar y mantener disponibles y operativos los servicios de IT. Las etapas en el mantenimiento y restauración de un servicio son:

- Anticipar fallas
- Detectar fallas (incidentes)
- Diagnosticar fallas (problemas)
- Resolver fallas (errores conocidos)
- Recuperarse de fallas.

Confiabilidad

Confiabilidad incluye llevar la pista, entender y anticipar fallas. Está determinado por:

- La confiabilidad de cada parte de la infraestructura
- La resistencia del servicio
- El nivel de mantenimiento preventivo.

Practicidad

Practicidad es el servicio y soporte suministrado por organizaciones externas. Algunas preguntas podrían ser:

- Las operaciones IT son dependientes de proveedores de servicio externo o vendedores para detectar problemas, llegar y arreglarlo o responsabilidad de mantenimiento?
- Cómo se controlan las dependencias de modo que la detección de problemas y el mantenimiento sean realizados a tiempo?
- Los problemas son escalados a vendedores externos para aislar el ticket de problema o resolución?

La administración de la disponibilidad acompasa todo lo que tiene que ver con el servicio entregado, directa o indirectamente. Esta disciplina nos da un vistazo a lo grande y expansivo que es realmente el universo de los sistemas altamente disponibles.

Administración de la seguridad

Una compañía basada en el conocimiento que depende en el flujo libre de la información entre todos sus empleados para que funcione su negocio, tiene un tremendo desafío de seguridad. Aplicar suficientes recaudos para que el negocio no sea dañado, y de modo que la propiedad intelectual y los datos propietarios no sean divulgados en Internet, necesita planificación. Además, la protección de la información personal de los clientes, y su seguridad se vuelve un problema complejo a resolver.
Seguridad es asegurarse de que una persona que use nuestro sistema esté autorizada a estar allí, sea quien dice ser, y tenga acceso sólo a ciertas áreas del sistema que se apliquen para su función. La administración de sitios altamente disponibles incluye actividades preventivas, monitoreo y la producción de reportes que contengan información específica de acuerdo a los requerimientos del negocio. Incluye además, asegurarse que los socios, empleados y contratados conocen las medidas de seguridad que se les aplica, y cómo implementarlas.
Se debe disponer de ambientes de seguridad para equipos y trabajadores.
Un sistema altamente disponible debe tomarse en serio el tema de seguridad. No importa si se

tiene equipamiento y aplicaciones redundantes para asegurarse que las cosas sigan funcionando si el personal de limpieza puede entrar y desenchufar el servidor web.

Uso de la Tecnología de la información para ganar ventaja competitiva

El rol de la tecnología de los sistemas de información ha ido evolucionando. Inicialmente la tecnología de la información (IT) era usada principalmente para llevar registros, contabilidad, almacenamiento de datos y para realizar tareas repetitivas. Hoy en día se está propagando a través de la cadena de valor, combinando tecnología y economía para realizar las denominadas "actividades de valor".
La tecnología de la información (IT) ha pasado de satisfacer las necesidades básicas de una empresa a tener un rol fundamental en la búsqueda de una ventaja competitiva.

Preguntas que una empresa debe hacerse (Mc. Farlan, Harvard University)

- La tecnología de la información puede construir barreras a la entrada? Para ello debe ser difícil de imitar.
- La tecnología de la información puede crear costos de cambiar de proveedor del servicio? Lo ideal es que la tecnología esté tan embebida en el negocio que sea muy costoso de cambiar de proveedor.
- La tecnología de la información puede cambiar la base de la competencia? IS debe verse como un área de oportunidad de bajar costos o agregar valor a los productos o servicios.
- La tecnología de la información puede cambiar el equilibrio de poder en las relaciones del proveedor?
- La tecnología de la información puede generar nuevos productos?

Si la respuesta a una o más de estas preguntas es SÍ, la tecnología de la información representa un recurso estratégico que requiere atención al mayor nivel.

Pasos que una empresa debe seguir para sacar partido de las oportunidades creadas por IT (Porter y Millar)

- Calcular la intensidad de la información de los productos y servicios
- Determinar el rol de IT en la estructura industrial: debe determinar el impacto que el uso de IT tendrá en su propia estructura industrial
- Identificar y ordenar las formas en las cuales IT podría conseguir una ventaja competitiva
- Investigar cómo IT podría generar nuevos negocios
- Desarrollar un plan para sacar partido de IT

Calidad

Concepto de calidad

Definición clásica

- adecuación al uso
- ajustarse a ciertas especificaciones o estándares

Aportes significativos al concepto de calidad:

Demming	Constancia de propósito Mejoramiento continuo Erradicar el temor	"Calidad es sobrepasar las expectativas y necesidades de los clientes a lo largo de la vida del producto"
Juran	Planificación de calidad Control de calidad Mejora continua	"Calidad es la adecuación al uso"
Crosby	Compromiso de la dirección Prevención Cero defecto Educación del personal Precio de la no calidad	"Calidad significa conformidad con los requisitos"

¿Qué es calidad? Proveer a los clientes externos e internos de productos y servicios que cumplan plenamente con sus requerimientos e incluso los anticipen, a un costo razonable y en el plazo acordado, logrando todo esto a través de un proceso de mejora continua.

Indicadores de éxito:

- satisfacción de los clientes
- satisfacción de los empleados
- menor necesidad de control
- mayor conocimiento de las distintas áreas por todo el personal
- menor costo de no-calidad (reprocesos, restauraciones, reprogramaciones, etc.)
- sistematización de procedimientos

- líder en el sector
- inversión continua en educación
- beneficios a largo plazo

Calidad en los servicios: bienes intangibles

Cada vez más, los países industrializados y en vías de desarrollo ven crecer cada vez más el sector terciario de la economía (el sector primario se refiere básicamente al agro, el sector secundario a la industria, y el terciario a los servicios). Esto se refiere no sólo a valores absoluto, sino también a la cantidad de empleos. Por esta razón es necesario plantearse si los modos de reflexión y decisión elaborados en el contexto de los productos están adaptados a los de los servicios.

¿Qué es un servicio?

Servicio, en este contexto, es un trabajo realizado para alguien más. El receptor del servicio (con frecuencia llamado cliente) puede ser:
- un usuario individual (consumidor)
- una institución (por ejemplo, una empresa que alquila una oficina)
- ambos (por ejemplo, usuarios de energía eléctrica de una fuente central)

El trabajo de servicios existe porque:
- permite que el cliente satisfaga necesidades que de otro modo no podría, como por ejemplo, comunicación de voz de larga distancia
- ofrece al cliente alternativas que son superiores por el costo, tiempo, conveniencia, etc., como por ejemplo, el transporte público
- cumple una amplia variedad de necesidades humanas, ya sea fisiológicas como psicológicas, como por ejemplo, entretenimiento, liberarlos de tareas desagradables, oportunidad de aprender y creatividad.

El trabajo de servicios puede incluir la venta de productos, como por ejemplo, la comida en un restaurante, repuestos durante la reparación de un auto. Sin embargo, esta venta es incidental al trabajo realizado para el cliente.
La definición de las industrias de servicio normalmente excluye la manufactura, agricultura, minería, y construcción, pero sí incluye:
- transporte público
- utilidades públicas (comunicaciones telefónicas, energía, sanidad)
- restaurantes, hoteles
- marketing (comida al por menor, mayoristas, supermercados, vestimenta)
- finanzas
- medios
- servicios personales (entretenimiento, lavandería, peluquería)
- servicios profesionales (abogados, científicos)
- gobierno (defensa, salud, educación, servicios municipales, asistencia social)

Comprender la naturaleza del acto de servicio:

¿Cuál es la naturaleza del acto de servicio?	¿Quién o qué es el beneficiario directo del servicio?	
	Las personas	**Las cosas**
Acciones tangibles	Servicios destinados a los cuerpos de las personas	Servicios destinados a bienes y a otras posesiones físicas
	• cuidados • transporte de personas • salones de belleza • gimnasios • restaurantes • salón de peluquería	• transporte de fletes • mantenimiento y reparación industriales • guardia • tintorería/lavandería • concepción/cuidado de los parques • cuidados veterinarios
Acciones tangibles	Servicios destinados a las mentes de las personas	Servicios destinados a posesiones intangibles
	• educación • programas de radio • servicios de información • teatros • museos	• bancos • servicios de ayuda legal • contabilidad • la Bolsa de Valores • seguros

Características de una empresa de servicios

Una compañía de servicios es un sistema de facilidades y habilidades especiales, organizadas para proveer servicios a clientes. Vende el beneficio de su sistema a sus clientes en una variedad de formas:

- renta, por ejemplo, alquiler de apartamentos
- uso de facilidades, por ejemplo, llamadas de teléfono
- consjeo profesional, por ejemplo, médico
- salud, por ejemplo, hospital
- mantenimiento de productos, por ejemplo, reparación de autos
- relevo de autoservicio, por ejemplo, servicio de restaurante.

Para llevar a cabo su misión, la empresa de servicios normalmente le vende servicio directamente al usuario. Esto hace que la compañía tenga contactos múltiples con numerosos consumidores, realizándose un número importante de transacciones. Todas ellas tienen impacto en los seres humanos. Un aspecto favorable de este contacto directo ese la oportunidad de tener retro-alimentación con respecto a la adecuación al uso. En esto la empresa de servicios tiene un trabajo más fácil que la empresa manufacturera, que, comparativamente está aislada del consumidor y debe recurrir a estudios especiales para asegurarse retro-alimentación adecuada.
El extensivo contacto personal también establece algunas relaciones que son inherentemente desagradables para el cliente, como por ejemplo, tener que hacer cola de espera para ser

atendido.

Servucción (Eiglier y Langeard)

Es el proceso de creación del servicio.

Elementos para una teoría de servucción

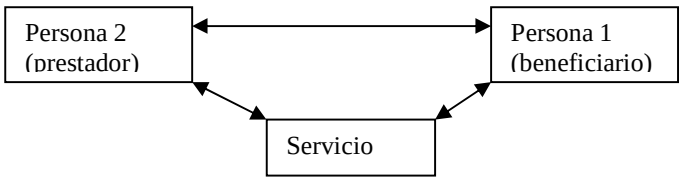
El instrumento para estudiar el concepto de servucción es la teoría de sistemas.

Propiedades de los sistemas (L. Von Bertalanfy)

- constituido por elementos identificables
- todos los elementos están relacionados entre sí
- funciona hacia un objetivo o finalidad
- ya sea un sistema cerrado o abierto, tiene una frontera identificable
- funciona tendiendo a un estado de equilibrio
- todo cambio o modificación de un elemento conlleva por el juego de interrelaciones, un cambio no directo del resultado del sistema

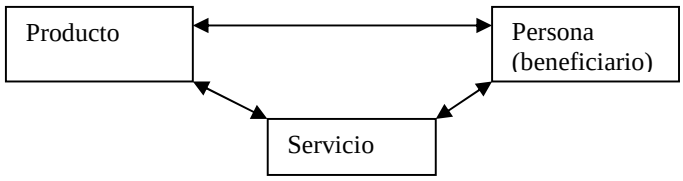
Tipos de sistema

Tipo 1



El servicio será evaluado como bueno o malo por el beneficiario, y esto afectará no sólo su comportamiento general sino también a sus relaciones futuras con el prestador. Este también evaluará el servicio según el trabajo que le dio, la molestia, y hasta su nerviosismo, lo que afectará sus relaciones con el beneficiario. Ambos pueden tener una evaluación diametralmente opuesta sobre la calidad del servicio. En conclusión, un mismo servicio producido por las mismas personas, no presenta una calidad estable en el tiempo.

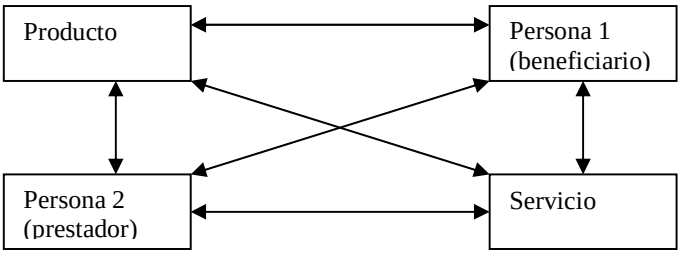
Tipo 2



Este sistema ilustra el consumo o utilización de un bien tangible. Al contrario que en el sistema anterior, los estándares de calidad objetivos son más fáciles de definir, porque participa una sola

persona. El funcionamiento de la máquina o del bien permanece estable en el tiempo.

Tipo 3



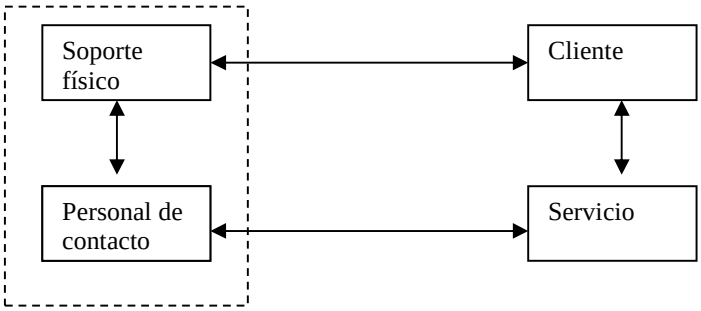
Ejemplo: la persona 1 (beneficiario), pide a la persona 2, un amigo (prestador), que lo deje en su coche (producto) en un lugar determinado. Las variables que pueden afectar la calidad del output (servicio en sí) son numerosas:

- naturaleza de cada uno de los elementos (las dos personas, el coche)
- la calidad de las informaciones que va a dar el beneficiario al prestador (R5), las respuestas de éste último (R8), y la conversación que se va a establecer entre ellos.
- La forma de conducir del prestador (R7), la utilización por el beneficiario de los instrumentos que tiene a su disposición en el coche (R4).
- Las posibilidades del coche en relación con las expectativas y solicitudes de cada una de las 2 personas (R1, R2, R3)
- Las expectativas de las dos personas de cara al servicio (R6, R9) así como sus evaluaciones (R11, R12)
- Las consecuencias del servicio sobre el desgaste del coche (R10).

Elementos	**Producto**	**Persona1**	**Persona 2**	**Servicio**
Producto		R4	R7	R10
Persona 1	R1		R8	R11
Persona 2	R2	R5		R12
Servicio	R3	R6	R9	

Equilibrio del sistema

En el sector no comercial, la producción de los servicios se basa generalmente en una permanencia de la relación entre los miembros. Esto permite la alternancia de las funciones para la producción de un mismo servicio, o la posibilidad de trueque de servicios (por ejemplo, entre varios compañeros de trabajo que son vecinos, se turnan para ir juntos en el auto de uno diferente cada vez)
En el sector comercial, ya no puede funcionar basándose en trueque, y aparece otra variable para apoyar el equilibrio: el *dinero*. En este caso, el prestador es siempre el mismo y el beneficiario lo es a cambio de dinero.Este en realidad es un equilibrio aparente, ya que los miembros tienden a querer romperlo. Así aparecen los efectos de dominación por parte de los prestadores, tratando de mantener la clientela cautiva, con la consiguiente insatisfacción de éstos.



La organización como sistema

Una organización es un sistema socio-técnico incluido en otro más amplio que es la sociedad con la que interactúa influyéndose mutuamente.
También puede ser definida como un sistema social, integrado por individuos y grupos de trabajo que responden a una determinada estructura y dentro de un contexto al que controla parcialmente, desarrollan actividades aplicando recursos en pos de ciertos valores comunes.

Subsistemas que forman la Empresa

a) *Subsistema psicosocial*: está compuesto por individuos y grupos en interacción. Dicho subsistema está formado por la conducta individual y la motivación, las relaciones del status y del papel, dinámica de grupos y los sistemas de influencia.
b) *Subsistema técnico*: se refiere a los conocimientos necesarios para el desarrollo de tareas, incluyendo las técnicas usadas para la transformación de insumos en productos.
c) *Subsistema administrativo*: relaciona a la organización con su medio y establece los objetivos, desarrolla planes de integración, estrategia y operación, mediante el diseño de la estructura y el establecimiento de los procesos de control.

Servucción de la empresa de servicios

Es la organización sistemática y coherente de todos los elementos físicos y humanos de la relación cliente-empresa necesaria para la realización de una prestación de servicio cuyas características comerciales y niveles de calidad han sido determinados.

Concepción de sistemas adaptados

Concepción del servicio

Para concebir el/los servicios a aprestar, debe tenerse en cuenta que la servucción es un sistema y debe ser pensado globalmente, teniendo en cuenta que lo más importantes es la satisfacción de las expectativas del cliente y la facilitación de su papel. Un servucción es más compleja que una fábrica en el sentido que, no se domina uno de los elementos del sistema que es el cliente.

Pasos

1. Definición específica del resultado que se pretende conseguir.
2. Identificación del tipo de elementos necesarios para la realización del servicio.
3. Decidir la naturaleza y el tipo de relaciones que van a darse entre estos elementos, de forma que faciliten el resultado deseado

Conceptos fundamentales

No es lo mismo la oferta (el servicio que la empresa pone en el mercado) que el soporte de la oferta (los elementos de la servucción que controla, el soporte físico y el personal de contacto). Por ejemplo, el servicio de un banco puede ser proporcionarle al cliente dinero en efectivo, y el soporte físico es el cajero automático. Ocurre lo mismo con el output o salida (resultado de la servucción, el servicio) y el proceso (las interacciones de funcionamiento de la servucción).

Segmentación de la clientela

Concebir un sistema de servucción adaptado y eficaz implica su especialización, es decir, su incapacidad para fabricar otro servicio, o servicios sensiblemente diferentes según lo que esperen los clientes que se presenten. Por lo tanto es importante identificar qué clientes queremos atender, o sea, segmentar o dividir la clientela: sólo debemos juntar personas cuyos gustos, deseos y comportamientos sean lo más homogéneos posibles. No sólo debemos clasificarlos sino también elegir uno de estos grupos para especializar la servucción en función de éste.

Decisiones importantes

- Criterios: además de los tradicionales socio-demográficos, importa la situación (por ejemplo, para el transporte aéreo y hotelería, el motivo del viaje)
- Elección del segmento: la política de segmentación es viable si se elige un amplio segmento, de modo que ésta no sea discutida cada 6 meses.

Capacidad

Determina el importe de la inversión, y por lo tanto, la rentabilidad. Implica determinar:

- Cuántas unidades de servicio por unidad de tiempo
- Cuántos clientes pueden ser atendidos en un día
- Cuántos clientes pueden ser atendidos al mismo tiempo

Factores:

- Los servicios no se almacenan: no se puede hacer stock para cubrir picos de demanda.
- Estacionalidad
- Competencia

Dimensiones de la Calidad de los servicios

A diferencia de la calidad de productos, la calidad de servicios no puede controlarse a priori, puesto que, la fabricación y el consumo del servicio son en general simultáneos. Esto impide el filtrado de la calidad que existe en la industria. Es decir, no se puede controlar la calidad de los servicios, y rechazar los que no alcanzan cierto estándar, antes de ponerlos en el mercado, como

en el caso de los productos tangibles. Además, el cliente cobra una importancia mayor, ya que puede actuar como productor y consumidor al mismo tiempo, del servicio.

Salida (Output)

Se trata de la calidad del resultado del proceso. Como toda calidad, la calidad de un servicio es relativa y debe compararse con algo: las expectativas del cliente.

Elementos del proceso de producción del servicio

- **Cliente**: importa el grado de participación requerida del cliente. Además, según el servicio, si tiene una actitud innovadora.
- **Soporte físico**: instrumentos necesarios para el servicio (objetos, muebles, máquinas puestos a disposición del personal de contacto y/o del cliente), y el entorno material en el que se desarrolla el servicio (todo lo que se encuentra alrededor de los instrumentos: los edificios, el decorado, etc.)
- **Personal de contacto**: personifica a la empresa a los ojos del cliente.
- **El servicio**: ejemplo, Atención de consultas a usuarios. Se pueden definir varios niveles: mantenimiento, asesoría, y hotline.

Esta calidad de los elementos de servucción se expresa en dos dimensiones:

- *Calidad intrínsica* de cada uno de ellos tomados aisladamente (soporte físico: limpieza, estado de mantenimiento; personal de contacto: presentación y disponibilidad, eficacia; el cliente: pertenencia al mismo segmento y eficacia de su participación)
- *Grado de coherencia* entre ellos y grado de adaptación al servicio buscado, y por lo tanto, a las expectativas del segmento.

Proceso

- fluidez, facilidad, eficacia – colas de espera => disponibilidad del personal

Acciones a favor de la calidad

- Medir: hacer un sondeo sistemáticos entre los clientes
- Controlar: debe realizarse a intervalos regulares pero bastante separados en el tiempo. Lo que se analiza es el soporte físico, personal de contacto, interacción con los clientes, siempre poniéndose en el lugar del cliente y sus necesidades y expectativas.
- Círculos de calidad: permite motivar al personal de contacto, canalizar energías innovadoras, lo que evita las evoluciones no controladas de la servucción.

Control de calidad

Definición

Estrategia para administrar cada etapa de la producción para reducir al mínimo los errores o eliminarlos.

La calidad puede ser una de las maneras más importantes de "agregar valor" a los productos y servicios y distinguirlos de la competencia. Por lo tanto en lugar de ser vista como una simple actividad de inspección, se le ve ahora como una parte integral de la estrategia de la compañía.
En un tiempo los administradores pensaban que había una contradicción entre productividad y calidad: para lograr una tenía que renunciarse a la otra.

Control de calidad tradicional

Se enfoca en identificar los errores más que prevenirlos:

- aceptación de la muestra
- control el proceso

Calidad total

Se refiere a la calidad no sólo del producto final, sino calidad en el proceso, calidad en todas las etapas y las áreas de la empresa.
Es una filosofía de gestión que da respuesta a los cambios que se están dando, y que intenta comprometer a todos.

¿En qué se basa la Calidad Total?

- Respeto mutuo, confianza => beneficio mutuo
- Liderazgo
- Educación
- Sistemas: de capacitación, de evaluación de desempeño, de administración de salarios
- Participación, involucramiento

Dificultades

- Resistencia de las personas
- Poder de la organización informal

Círculos de calidad

Grupos de trabajo que se reúnen para analizar cómo se puede mejorar la calidad, y resolver problemas de la producción.

Administración de calidad total

Es el compromiso estratégico para mejorar la calidad combinando métodos estadísticos de control de calidad con un compromiso cultural de buscar incrementos en las mejorías que eleven la calidad y bajen los costos.
Con esta filosofía, la calidad no se controla, sino que se ejerce, y también se programa.

Implementación de un programa de Administración de la Calidad

Hay 3 prerrequisitos fundamentales para implementar un programa de Gerenciamiento de la Calidad dentro de una organización:

1. Compromiso (Commitment)
2. Cultura
3. Costo

El Gerenciamiento de la Calidad no es una extensión de otras iniciativas relacionadas con la calidad, pues trasciende la función de calidad en administración estratégica y de procesos.
Alcanza a las personas, clientes, proveedores, y sociedad, además del énfasis tradicional en el desempeño financiero.

Los gerentes de la organización no sólo deben controlar sino que también deben liderar, mostrando compromiso, deben desarrollar una cultura conmensurada con su visión y misión, y además, proveer los fondos para la implementación del programa.

La evolución del concepto de Calidad introdujo a principios de los ’90 el acrónimo TQM (Total Quality Management), pero aún hoy sigue habiendo confusión con el concepto de QA (Quality Assurance).
En realidad QA tiene que ver con la calidad de productos y servicios mientras que TQM abarca toda la organización.
QMS (Quality Management Systems) o QM, es una denominación más reciente, que surgió para enfatizar la necesidad de enfocar la calidad como una parte integral de las actividades de administración o gerenciamiento dentro de la organización.
La implementación exitosa de un programa de QM debe incluir no sólo entrenamiento en un conjunto de técnicas de QA, y también una re-calibración de la forma de pensar de la organización.
La mejora en el desempeño, calidad del producto y servicio son resultados específicos que también justifican QM.

	QA	QM	Directivas QM
Enfoque	Garantía al cliente	Satisfacción de propietarios, clientes, empleados,	Responsabilidad social

		proveedores y sociedad	
Motivación	Impuesta externamente	Generado internamente	Liderazgo de administración
Areas de aplicación	Funciones de línea relacionadas a la producción	Organización entera	Alcanza a toda la compañía
Participantes claves	Profesionales de calidad, gerentes y personal de línea	Todos los gerentes y empleados	Involucramiento en todos los niveles
Directivas principales	Prueba de conformidad del producto y sistema de QA	Mejora continua de proceso y producto	Cultura de la compañía de hacer correctamente las cosas correctas
Meta	Participar en el mercado, o Ventaja de mercado	Resultados globales del negocio y competitividad	Enfoque de costo de la calidad

La última columna describe los factores críticos de éxito: compromiso, cultura y costo.

Compromiso

El compromiso para QA está relacionado con la retención de los clientes y el lucro. QM se basa en el reconocimiento que la administración tiene responsabilidades sociales con todas las partes involucradas (dueños, clientes, empleados, proveedores y sociedad).

Compromiso desde arriba

Es la responsabilidad de la dirección establecer las estrategias para lograr los objetivos de la organización y establecer prioridades para alcanzarlos.
Es difícil de convencer a los administradores de adoptar esta filosofía puesto que los beneficios de la implementación de QM son tangibles a largo plazo.

Compromiso de los recursos de la organización

Una de las primeras prioridades es el entrenamiento de ciertos gerentes y personal clave que serán los facilitadores de la implementación del QM. Por tanto el compromiso inicial de recursos es para el entrenamiento y también reservar tiempo para hacer un seguimiento de los proyectos de QM.
Los facilitadores:

- Deben guiar a los otros a lo largo de varios pasos que estarán en línea con las necesidades y prioridades de la organización.
- También deben controlar el nivel de preparación de los empleados en el uso de las herramientas de calidad, para asegurar capacitación cuando se necesite. Esto es importante para evitar la frustración de no saber cómo manejar situaciones no familiares, y la subsecuente pérdida de entusiasmo.

- Deben controlar los proyectos de QM para evitar sub-optimización de la organización

Compromiso del tiempo de los administradores o gerentes

No basta con la mera aprobación de embarcarse en un proyecto de QM sino que debe demostrarse liderazgo a través de la participación activa.

Cultura

Cooperación y trabajo en grupo son ejemplos que logran sinergia por la asociación de varias funciones.
Los signos de una organización que aprende son: respeto de todos los individuos, estímulo a la innovación, énfasis en la mejora en vez de los errores cometidos.

Mejora continua

Debe proveerse a la organización de la mejor administración de crisis en áreas con problemas y desarrollar un personal que busque activamente oportunidades de hacer las cosas de una mejor manera, para evitar la repetición de problemas. Hay una gran diferencia en costo entre corregir y prevenir. QA se basa en la prevención y corrección de problemas. QM busca activamente oportunidades de mejorar revisando aspectos que pueden no aparecer como problemáticos.

Manejo de los cambios

Existe la filosofía “eso no se inventó aquí, por lo tanto no es bueno para nosotros” y también “siempre se hizo de esta manera”, que son incompatibles con QM, puesto que esta se basa en buscar la manera de hacer mejor las cosas, es decir, en el cambio permanente. La voluntad de las personas de aceptar los cambios es esencial para implementar QM.

Trabajo en grupo y respeto mutuo

QM provee la oportunidad de beneficiarse de gente trabajando junta en una misma dirección. La habilidad de una organización de convertir la diversidad entre sus empleados en fuerzas complementarias es otro indicador del nivel de madurez de un programa de QM.
La claridad de propósito es esencial en un grupo de trabajo para evitar conflictos de prioridades y objetivos dispares. Es necesario tener habilidades de comunicación e implementar técnicas de construcción de equipos.
También es necesario el respeto mutuo. No se puede pretender que toda idea innovadora sea exitosa. Por tanto, es importante erradicar el miedo al ridículo o al castigo. Los errores cometidos deben tomarse como una oportunidad de aprendizaje.

Enfoque analítico

QM no es una solución mágica sino que requiere trabajo arduo y disciplina para analizar una situación y establecer medida apropiadas para resolver una cuestión particular, y más aún para realizar mejoras.
QM tiene un enfoque analítico frente a cualquier situación, ya sea orientada a personas o de naturaleza técnica, y luego de establecer las mediciones debe compararse con alguna referencia.

Costo

Las organizaciones de hoy en día deben controlar muy de cerca sus costos. Por eso es frecuente que la gerencia asigne menor prioridad a los proyectos de calidad debido a restricciones financieras. Irónicamente estas son las ocasiones en que se presentan las mayores oportunidades de minimizar pérdidas operativas siguiendo proyectos de mejora de calidad racionales.

Enfoque de valor agregado

El enfoque del control de calidad y financiero es minimizar las ineficiencias y los gastos innecesarios.
Los gerentes pueden usar un enfoque QM para hacer que los empleados vean qué beneficios están aportando para los clientes. Este punto de vista se adapta bien al enfoque QM orientado al cliente, mientras que las prioridades y actividades diarias están alineadas con los objetivos corporativos de mejorar la eficiencia operacional y los niveles de servicio al cliente.

Justificación de los proyectos de QM

Todo proyecto de QM debe analizarse para establecer su relevancia con respecto a las metas y prioridades organizacionales y en relación con el retorno sobre la inversión esperado.

Justificación de un programa de QM

La implementación de QM requiere una inversión en entrenamiento y tiempo. La retribución está en las mejoras en eficiencia y en calidad de producto y servicio. Además, los resultados combinados a largo plazo de un programa de QM exitoso, excelencia en el pensamiento y métodos de trabajo de alta calidad permiten que la organización sea más dinámica y adaptable, y por tanto, competitiva.

Calidad en la gestión de un Centro de Cómputos

Dimensiones: grado creciente de refinamiento

- Nivel primario:
  - Provisión de sistemas de software para manejo del negocio
  - Provisión del soporte físico para los sistemas de información
- Atención a usuarios
- Continuidad de disponibilidad del servicio informático
- Adaptabilidad y rapidez de introducción de nuevas tecnologías como apoyo al negocio
- Confiabilidad y seguridad de los sistemas
- Aprobación de auditorías
- Información de apoyo a la toma de decisiones gerenciales

- Definición de estrategia ante contingencias

Clases de pérdida de efectividad:

- Gastos innecesarios: tiempo (cuánto cuesta una reunión inefectiva), desperdicio de materiales, servicio
- Subutilización de activos: físicos (equipos, inventario), financieros (cuentas a cobrar, intereses perdidos), humanos (tiempo y talento de las personas)
- Tiempos de respuesta lentos: tareas atrasadas (falta de información, necesidad de revisión)
- Pérdida de ventas y oportunidades

Calidad de datos y Calidad Total

Calidad de datos	Características	Métricas
Exactitud	Datos sin errores	% de valores completos comparado con el valor real. Por ejemplo, M=masculino cuando así lo es en la realidad
Completitud	Grado en que están presentes los valores en campos que lo requieren	% de campos de datos a los que se les ingresó valor
Consistencia	Grado en que un conjunto de datos satisface una restricción	% de valores que cumplen una restricción de existencia en tablas/archivos/registros
Oportunidad	Grado en que un conjunto de datos está actualizado	% de datos disponibles dentro de un período específico (días, horas, minutos)
Unicidad	Estado de ser el único de su clase	% de registros con clave primaria única
Validez	Calidad de datos encontrado en un sistema adecuado de clasificación, y que es suficientemente riguroso como para llevar a la aceptación	% de datos que tiene valores dentro de su respectivo dominio permitido

En este objetivo de conseguir una alta calidad de datos se pueden aplicar técnicas de Administración de Calidad Total (TQM) en lo que llamaremos Administración de Calidad Total de Datos (TDQM), integrando técnicas administración de personal y métodos cuantitativos para mejorar productos y/o servicios. Esto significa combinar técnicas de administración funcional con esfuerzos de mejora, y herramientas técnicas de una forma disciplinada y enfocada a crear y sustentar un compromiso de mejora continua.

Pasos

1. Establecer un ambiente TDQM
   Esto significa el trabajo en grupo del área funcional y la gente de TI, con sus naturales barreras de comunicación y diferentes puntos de vista.
2. Desarrollar un plan estratégico
   Este plan debería contener: objetivos y metas para la administración de calidad de datos, estrategias y proyectos para conseguir estas metas y objetivos, objetivos de calidad de datos medibles.
3. Desarrollar y administrar una cultura
   La infraestructura a generar necesita conseguir responsabilidades organizacionales, establecer programas de entrenamiento, abrir líneas de comunicación entre los expertos funcionales y los profesionales de TI.
4. Establecer alcance del proyecto de calidad de datos y desarrollar el plan de implementación
   Los objetivos principales son: identificar los proyectos de calidad de datos que sean factibles implementar, y desarrollar los planes para implementarlos.
5. Identificar los proyectos de calidad de datos
   Típicamente, los usuarios funcionales presentan los proyectos basados en sus frustraciones con respecto a errores en los datos de tablas y/o registros. Los administradores de sistemas pueden hacer recomendaciones basados en problemas conocidos en la recolección de datos, errores de proceso y procedimientos internos de validación de datos. Otros factores que pueden incidir en la selección de los proyectos de calidad de datos pueden incluir enfocarse en áreas de mayor oportunidad de éxito y de prototipar/mostrar el valor de los esfuerzos de calidad de datos para convencer a los gerentes. Esto es importante puesto que el éxito o fracaso de los proyectos iniciales pueden condicionar el comportamiento de la organización en cuanto a adoptar o no las ideas de TDQM.
   Para elegir proyectos que tienen oportunidad de éxito, conviene seleccionar los proyectos que:
   - Tienen la mayor probabilidad de éxito
   - Tienen los mayores costos de errores
   - Se pueden mejorar significativamente

   Para elegir proyectos que requieran poco esfuerzo de prototipado: si no hay apoyo de la gerencia, realizar una demostración. Elegir un proyecto que:
   - Tenga bajo riesgo y poca visibilidad cuyo éxito sea crítico para la administración.
   - Enfocarse en datos familiares a los expertos del área funcional y/o de TI
   - Seleccionar un esfuerzo inicial que no sea demasiado grande de modo que no esté predestinado al fracaso, ni tan pequeño como para que las mejoras pasen desapercibidas
6. Desarrollar el plan de implementación de calidad de datos
   Los planes de implementación proveen información sobre:
   - Resumen de tareas: lista de objetivos del proyecto, alcance y beneficios esperados
   - Descripción de tareas de calidad de datos
   - Enfoque del proyecto: tareas y herramientas a utilizar
   - Cronograma: identifica el inicio, fechas de finalización y mojones
   - Qué se entrega: reportes y/o productos que documenten el resultado (estado inicial de la calidad de datos, reporte técnico que fundamente las mejoras, descripción de las acciones implementadas para obtenerlas
   - Recursos necesarios para completar el proyecto

7. Implementar los proyectos de calidad de datos
   Actividades:
   - Definición: identificar los requerimientos de calidad de datos y establecer métricas. Se necesita una análisis de problemas históricos de datos, identificar y revisar la documentación de TI, identificar las reglas de negocio.
   - Medición: medir conformidad con reglas de negocio establecidas y desarrollar reporte de excepciones. Esto implica analizar la naturaleza y magnitud de problemas de datos que tienen los valores realmente almacenados en tablas. Para ello se compara con estándares, ejecutando un conjunto de reglas (por ejemplo sentencias SQL que extraigan la cantidad de registros que no cumplen una cierta restricción).
   - Análisis: verificar, validar y asegurarse de las causas de la pobre calidad de datos y analizar oportunidades de mejora. Para ello se necesitan los reportes de métricas, y también el apoyo de los expertos del área funcional. Es necesario identificar los problemas clave de datos, sus causas, los costos que acarrearían el solucionarlos, y soluciones para mejorar los procesos que se utilizan para crear y mantener los datos libres de errores.
   - Mejora: seleccionar las oportunidades de mejora de calidad de los datos que provean los mayores beneficios e implementarlos. Esto puede llevar a cambiar los procedimientos de ingreso de datos, y las reglas de validación de los mismos.
8. Evaluar el proceso de administración de calidad de datos
   Esto refuerza la idea de que TDQM no es una forma programada de hacer negocio. Se necesita que los participantes revisen los procedimientos existentes de control de calidad de datos y determinen dónde, los proyectos de calidad de datos han ayudado a mejorar.

La calidad de datos en ambientes cliente/servidor

Las mejoras en la calidad de datos aumenta el valor de los sistemas de información de las organizaciones.
¿Por qué?:

- Ayuda a mejorar la calidad de las decisiones gerenciales y la eficiencia de las operaciones
- Aumenta la confianza de los auditores en la estructura de control interna y en la exactitud de los estados financieros
- En consecuencia, reduce los costos de auditoría, control de riesgo y testeo.

Un número creciente de organizaciones están haciendo reingeniería de sus sistemas, convirtiendo sus sistemas de plataformas mainframe a ambientes cliente/servidor. Aunque se dedican muchos recursos al desarrollo y mantenimiento de estos sistemas, los problemas de calidad de datos se agudizan en ambientes distribuidos. Presentaremos algunas guías para ayudar a los administradores de bases de datos, administradores de datos, y propietarios de los mismos, a mejorar la calidad de los datos, en cuanto a exactitud, relevancia, y disponibilidad en tiempo y forma.

Calidad de datos a nivel de tablas

Existe un marco de referencia para manejar la calidad de datos en sistemas de información para bases de datos completas. Se puede ver el proceso de convertir datos en decisiones, como análogo al proceso de convertir materias primas en productos terminados. De este modo se asume un enfoque de manejo de calidad de datos centralizado, utilizando conceptos de control de calidad en la fabricación. Sin embargo es necesario adaptarlo al ambiente de proceso de datos distribuido. Por ejemplo, errores en la entrada de datos incide mucho más en la calidad de las decisiones que los defectos de las materias primas sobre los productos terminados.
Por eso se hará hincapié en un enfoque de calidad de datos a nivel de tablas individuales:

- Las bases de datos distribuidas aumentan la probabilidad de que las tablas estén en los clientes en diferentes ubicaciones físicas y funcionales
- Es mejor dividir la responsabilidad de la calidad de los datos en un sistema de información completo, especialmente cuando los errores deben ser corregidos dentro de un corto plazo, pues de esta manera se divide el trabajo en unidades manejables.
- El enfoque a nivel de tablas proporciona un método de modularizar responsabilidades y control. Las responsabilidades se pueden asignar a personas con mejor acceso a las entidades que el sistema de información está modelando.

Procedimiento

- *Designar un propietario para la aplicación*: estas personas deben asegurar que los controles de entrada de datos son efectivos e identificar posibles mejoras. Por otra parte, deben tener la autoridad suficiente como para corregir situaciones anómalas. Necesitan entrenamiento adecuado y recursos para implementar y coordinar el resto de los pasos. Además, deben cooperar en resolver problemas de otras tablas porque normalmente están interrelacionadas.
- *Implementar controles de entrada de datos*: incluye chequeo de campos, de registros, de lotes de registros, o chequeo de archivos. Por ejemplo, para asegurar que en un campo se ingresen datos correctos, se presenta una lista desplegable de los valores válidos (ComboBox, check box, radio buttom, etc.). Controles al final de un formulario pueden invocar procedimientos que actualicen múltiples copias de los datos en ambientes distribuidos, o que hagan el “commit” o “rollback” de la transacción.
- *Monitorear la calidad de las transacciones de entrada*: ayuda en la etapa inicial de diseño de sistemas porque resulta imposible predecir todos los casos de error posibles. Cambios en la estructura de datos, las decisiones (nuevas reglamentaciones) o la configuración cliente/servidor pueden causar errores. Nuevas tecnologías pueden cambiar la naturaleza de los métodos de captura de datos, cambiando entonces radicalmente el tipo de controles a realizar. Por otro lado, como las empresas están dejando de usar los documentos en papel, el control automatizado es cada vez más importante.
- *Monitorear la calidad de los datos existentes*: una buena técnica es introducir “marcas” en los datos, como por ejemplo, la fecha y hora de modificación, y el usuario que lo hizo.
- *Desarrollar procedimientos para identificar errores de datos*:
  - correr procedimientos fuera de las horas pico de trabajo, en los que se realizan los controles de integridad referencial: Supongamos el caso de una orden incompleta de un cliente cuya cuenta fue cancelada luego de que la orden fuera ingresada.

  - Realizar chequeos para detectar problemas relacionados con fechas: por ejemplo una persona ingresa una requisición de materiales que luego nunca es ordenada.
  - Chequear casos de uso intensivo de registros, para sacar de línea esos procesos: por ejemplo, cálculos estadísticos, que deben recorrer tablas enteras y varias veces, deberían hacerse fuera de las horas pico.
  - Chequeos que involucran grupos de registros: por ejemplo, detectar diferencias entre las cantidades compradas y las recibidas.
- *Desarrollar técnicas para clasificar errores de acuerdo a sus potenciales consecuencias*: ayuda a establecer prioridades para la resolución de problemas.
- *Desarrollar procedimientos para determinar valores correctos de datos*: podemos clasificar las tablas en acumuladas (por ejemplo inventarios, cuentas a cobrar), que contienen registros permanentes, y tablas transitorias (por ejemplo, ventas, recibos), que contienen información transaccional. Los errores en el segundo grupo se propagan a las tablas permanentes, por lo que hay que desarrollar procedimientos para corregir las permanentes. Por ejemplo, realizar inventarios físicos completos, corrigen problemas de stock. Estimar cuentas a cobrar puede no ser tan fácil (involucra ventas, órdenes en curso, plazos de pago y puntualidad, probables ajustes, y variaciones en la tasa de cambio)
- *Usar controles de proceso estadísticos para determinar áreas con problemas*: el principio de Pareto declara que los mayores progresos en la calidad de datos pueden realizarse atacando unos pocos problemas que causan los errores de decisión más costosos. Esto sirve para maximizar el beneficio obtenido para el esfuerzo realizado.
- *Aplicar nuevas tecnologías de información*: por ejemplo, el uso de lectores de código de barras ha reducido drásticamente la cantidad de errores de entrada de datos, y los costos de ingreso.

Seguridad y control interno

¿Qué es la seguridad?

- Conjunto de medios que aseguran el correcto funcionamiento de alguna cosa.
- Conjunto de medios (normas, procedimientos, controles, dispositivos, etc.) destinados a proteger la organización y sus recursos de diferentes tipos de amenazas.

¿Qué es el control interno?

Proceso llevado a cabo por el Directorio, la Gerencia, y el Personal de una entidad, diseñado para proveer un aseguramiento razonable en relación al logro de los objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de los reportes financieros
- Cumplimiento de las leyes y regulaciones aplicables

Objetivos del control interno

- Resguardo de activos: ¿cuánto vale un archivo de deudores?
- Asegurar concordancia con políticas corporativas y requerimientos legales
- Autorización de ingreso de datos: ¿quién puede anular una transacción?
- Integridad y exactitud de las transacciones
- Salida adecuada
- Confiabilidad de los procesos
- Respaldo y recuperación
- Eficiencia y economía de los procesos

Objetivos de control en Sistemas de Información

- Control de acceso
- Autorización e ingreso único
- Integridad
- Proceso de transacciones rechazadas: a dónde van, quién es el responsable, se generan mensajes al administrador, etc.
- Proceso de transacciones duplicadas
- Respaldo y recuperación
- Proceso de aprobación de cambios en las aplicaciones y datos

Procedimientos de control de Información

Los clasificamos en las siguientes áreas:

- Procedimientos de control de organización general
- Acceso a datos y programas
- Metodología de desarrollo de sistemas
- Operación de procesamiento de datos
- Funciones de programación de sistemas y soporte técnico
- Procedimientos de control de Calidad de Procesamiento de Datos.

Autoevaluación de controles (ADC)

Es un proceso formal y documentado en el cual la dirección y/o el equipo de trabajo involucrado directamente en una función de negocios evalúa la efectividad del proceso, y decide sobre la probabilidad de alcanzar los objetivos.
Una de las características de la ADC es reforzar el control interno, extendiendo algunas de las responsabilidades de monitoreo al cliente, lo cual implica confiar que el cliente informa sobre sus propias debilidades.

ENFOQUE TRADICIONAL	**ENFOQUE ADC**
Asignar tareas y supervisar	Administrativos con poder de toma de decisión => mayor responsabilidad
Definición de políticas y reglas de manejo	Mejoramiento continuo
Participación y entrenamiento limitado a algunos empleados	Participación y entrenamiento extensivo
Analistas de control primario son los auditores	Analistas de control primario son los propios empleados

Debilidades del enfoque tradicional

- Se cree que los auditores son los únicos responsables por el control
- No se puede demostrar efectivamente que se realice alguna clase de control interno
- No es eficiente ni efectivo, puesto que su objetivo no es mejorar la eficiencia o efectividad corporativa, ya que muchas veces, la auditoría no tiene un alcance global, y quedan fuera áreas que podrían tener impacto.
- Se cree que más controles siempre son preferibles a menos controles, sin importar el área ni los objetivos.
- Se hace hincapié en áreas no siempre muy relevantes, como control de firmas, conciliación de saldos, en vez de entrenamiento, prácticas de contratación, etc.
- Remarca los síntomas y no las causas
- Es opuesto al enfoque de calidad total, en el cual disminuyen los controles, y crece la responsabilidad y participación de todos los empleados, a todos los niveles.
- No se acompasa a los cambios de las empresas de hoy en día: la globalización, la adquisición y fusión entre empresas (cada una con sus propias normas de controles).

Autoevaluación de controles y riesgo

Es el proceso que permite que grupos de trabajo identifiquen o mejoren los objetivos de negociación y calidad, y mide la efectividad de los planes y controles que se están llevando a cabo para cumplirlos.

Seguridad, control y reingeniería

En el momento en que se realiza la reingeniería de algún proceso de la organización, es una buena oportunidad para evaluar la seguridad y los procesos de control asociados a los nuevos sistemas de información, puesto que se puede aprovechar para establecer una nueva visión de los procedimientos de control.

Clasificación del riesgo (importancia de la información vs. grado de control)

Clasificación de la Información:

- *Vital:* no disponer de ella inhabilita la operativa normal con pérdida financiera definitiva (dependencia total del sistema)
- *Sensible:* su ausencia afecta la imagen de la empresa, sin originar pérdida financiera de consideración (pérdida parcial)
- *Importante:* su ausencia provoca distorsiones en la operativa normal, pero no origina pérdida de imagen ni de recursos, y es fácilmente recuperable.
- *Normal:* la información restante.

Clasificación del riesgo según la importancia de la información, y el grado de control:

CLASIFICACIÓN DE LA INFORMACIÓN

GRADO DE CONTROL	Vital	Sensible	Importante	Normal
Fuerte	Riesgo bajo	Riesgo bajo	Sin valor	Sin valor
Satisfactorio	Riesgo bajo	Riesgo bajo	Sin valor	Sin valor
Con deficiencias menores	Riesgo medio	Riesgo medio	Riesgo bajo	Riesgo bajo
Con grandes deficiencias	**Riesgo alto**	**Riesgo alto**	Riesgo medio	Riesgo bajo
Inaceptable	**Riesgo alto**	**Riesgo alto**	**Riesgo alto**	Riesgo medio

En el área de desarrollo de nuevas aplicaciones, esto ayudará a ahorrar tiempo y dinero en cambios posteriores.

Los requerimientos que se impongan en la etapa de análisis y diseño, permiten definir procedimientos de control apropiados, documentación adecuada de los sistemas, documentación de usuarios, procedimientos administrativos, y un conjunto de pruebas completo y documentado.
Antes de poner en producción una nueva aplicación, deberá entrenarse al usuario, definir los procedimientos de respaldos de la información y procedimientos alternativos en caso de contingencias.

Clasificación de la información: Una implementación corporativa

Clasificar la información corporativa basándose en el riesgo del negocio, valor de los datos y otros criterios tiene sentido para el negocio. No toda la información tiene el mismo valor o uso, o está sujeta a los mismos riesgos. Por lo tanto, los mecanismos de protección, procesos de recuperación, etc., deberían ser diferentes, con diferentes costos asociados.
La razón de la clasificación de los datos es bajar los costos de protección de los mismos, y mejorar la calidad del proceso de toma de decisiones de la corporación entera, ayudando a mejorar la calidad de los datos sobre los cuales dependen los decisores. Los beneficios de la clasificación de datos a nivel de la empresa, se obtienen a nivel corporativo, y no a nivel de una aplicación individual o departamental.

Beneficios

- Mejora en la confidencialidad, integridad y disponibilidad debido al uso apropiado de controles en toda la empresa.
- La organización saca el mejor provecho de su inversión en protección de la información porque los mecanismos de protección están diseñados e implementados donde más se necesitan, y los controles menos costosos pueden usarse en lugares donde la información no es crítica.
- Mejora en la calidad de las decisiones por la mejora en la calidad de los datos en que se basan.
- La compañía dispone de un proceso para rever todas las funciones del negocio y requerimientos de información periódicamente para determinar prioridades y valores de funciones y datos críticos del negocio.
- Se provee implementación de una arquitectura de seguridad de la información, que ubica mejor la compañía para futuras adquisiciones o fusiones.

Hay costos asociados con este proceso, pero la mayoría son costos por única vez, de puesta en marcha del programa, y una vez que está implementado, los ahorros compensan con creces.

Preguntas a responder

- ¿Hay un promotor del proyecto a nivel ejecutivo? Esto puede ser importante para derribar barreras y obtener apoyo de otros en la organización.
- ¿Qué se intenta proteger y de qué? Se deberá realizar una matriz de análisis de amenaza/riesgo para determinar cuáles son las amenazas, los riesgos asociados, y la información sujeta a esas amenazas.
- ¿Existen requerimientos legales?

- ¿El negocio ha aceptado responsabilidad de la propiedad de la información? La empresa, y no el departamento de IT es la propietaria de los datos. Las decisiones con respecto a quién tiene y qué acceso, qué clasificación asignar a los datos, deben ser tomadas por los propietarios de los datos del negocio. IT proporciona la tecnología y los procesos para ayudar a los propietarios de los datos.
- ¿Están los recursos adecuados disponibles para el proyecto inicial? No sólo la persona de IT.

Herramientas

- *Política de seguridad de la información*: Una buena herramienta para establecer un esquema de clasificación de los datos es tener una política corporativa que declare la información como un activo de la corporación a proteger. Además este documento debe decir que la información se clasificará según su valor, sensibilidad, riesgo de pérdida o compromiso, y requerimientos legales de retención. Esto le da al responsable de implementar el plan la autoridad para iniciar el proyecto y llevarlo adelante.
- *Política de administración de datos*: esta política debe establecer la clasificación de la información como un proceso para protegerla y definir:
  - Declarar a los gerentes locales como propietarios de la información
  - Definición de cada categoría
  - Criterios de seguridad para cada categoría, para datos y software:mínimo rango de controles a establecer para cada categoría
  - Roles y responsabilidades de cada grupo encargado de implementar la política o utilizar los datos
- *Procedimientos, procesos y estándares:* Además, debe haber un conjunto de procesos, procedimientos y estándares para implementar estas políticas, definidos a un nivel operacional. Estas son porciones "mecánicas" de las políticas y representan las actividades del día a día. Esto incluye:
  - Proceso para realizar un análisis de impacto del negocio (AIN)
  - Procedimientos para clasificar la información, inicialmente luego de terminar el AIN y también para cambiarlo posteriormente, si cambian las necesidades del negocio.
  - Proceso para comunicar la clasificación a IT de forma que puedan implementar los controles a tiempo de acuerdo a la clasificación de los datos que se haya definido.
  - Proceso para revisar periódicamente:
    i. Clasificación actual para determinar si aún es válida
    ii. Derechos de acceso actuales de individuos y/o grupos a un recurso en particular
    iii. Controles en efecto para una categoría, para determinar su efectividad
    iv. Requerimientos de entrenamiento para nuevos propietarios de datos
  - Procedimientos para notificar a los responsables de los datos, de cualquier cambio en los derechos de acceso de individuos o grupos.

Además de las políticas, el responsable del proyecto debe contar con el apoyo del departamento Legal y Auditoría Interna.

Análisis de Impacto en el Negocio

Esto se debe realizar a alto nivel, en las funciones principales dentro de la compañía. Este

análisis es usado por el equipo de trabajo para:
- Identificar las principales áreas funcionales de información (por ejemplo, RRHH, finanzas, investigación y desarrollo, marketing)
- Analizar las amenazas asociadas a cada área funcional. Esto puede ser tan simple como identificar riesgos asociados con la pérdida de confidencialidad, integridad o disponibilidad, o ir más en detalle con amenazas específicas de virus de computadoras, etc.
- Determinar el riesgo asociado con cada amenaza.
- Determinar el efecto de la pérdida del activo información en el negocio (estos pueden ser impacto financiero, regulatorio, de seguridad, etc.) para períodos específicos de no disponibilidad (1 hora, 1 día, 1 semana, etc.)
- Construir una tabla detallando el impacto de la pérdida de la información
- Preparar una lista de aplicaciones que sostienen directamente la función del negocio

A partir de la información recogida el equipo de trabajo puede identificar amenazas comunes a todas las funciones. Esto puede ayudar a poner las aplicaciones en categorías específicas con controles comunes para mitigar riesgos comunes. Además de las amenazas y los riesgos asociados, para clasificar también debe tenerse en cuenta la sensibilidad de la información y la facilidad de recuperación.

Establecimiento de categorías

Debe establecerse cuántas categorías habrá, y los controles necesarios para cada una. Además, se determinarán las responsabilidades y roles de los que estarán involucrados en el proceso. Demasiadas categorías sería poco práctico de implementar, y confuso para los propietarios de los datos, lo cual generaría resistencia. Por el contrario, pocas categorías sería percibido como que no valdría la pena el trabajo de desarrollarlas, implementarlas y mantenerlas.
Cada clase o categoría debe tener características fácilmente identificables, además deben ser disjuntas (lo máximo posible).

Ejemplo

- Público – la información que se muestra fuera de la compañía no dañará la organización, sus empleados, clientes o socios de negocios.
- Uso interno solamente – información que puede conocer cualquiera dentro de la organización pero dañaría a la empresa si es publicada fuera.
- Confidencial para la compañía – información que requiere “necesidad de saber” para tener acceso.

Es importante notar que los controles deben aplicarse a la información y al software. No basta con controlar sólo la información, el software y posiblemente el hardware donde reside deben asegurarse.

Controles claves

Podemos clasificarlos en:
1. Controles de detección

2. Controles preventivos
3. Controles correctivos

Hay también otra forma de ver los controles:

1. Controles básicos: controles de edición por programa/manuales, conciliación de totales de control de archivos y procedimientos de respaldo y recuperación
2. Controles disciplinarios: segregación de tareas, restricción física/lógica de acceso, y autorización de transacciones.

Controles mínimos de la información

- Criptografía – los datos son codificados con una clave para que no sean legibles. Esta clave debe mantenerse segura y sólo deben conocerla quienes tienen acceso autorizado a los datos. Puede considerarse los algoritmos de clave pública o privada para máxima seguridad y facilidad de uso.
- Revisión y aprobación – Debe existir un control de procedimiento de cambio de datos a realizar por alguien con conocimientos técnicos. Este control debe ser realizado por una persona diferente a quien realizó el cambio.
- Respaldo y recuperación – dependiendo de qué tan crítica sea la información y la facilidad de recuperación, puede ser necesario desarrollar planes especiales y probarlos periódicamente para asegurarse de que los datos se están respaldando bien y pueden recuperarse.
- Segregación de tareas – la idea es que ninguna persona tiene el control total sobre el ingreso de datos y el proceso de validación, para evitar que alguien pueda cometer fraudes o dañar a la organización. Por ejemplo, no debería permitirse que la misma persona creara vendedores en un archivo de vendedores autorizados, y además, pudiera autorizar pagos a vendedores.
- No debe existir acceso universal – Nadie tiene acceso a los datos a menos que se haya otorgado autorización específica para leer, actualizar, etc. La autorización para actualizar datos debe otorgarse a individuos, programas o transacciones específicos. Lo mismo se aplica para borrar información; cierto conjunto de individuos y/o programas serán los únicos que podrán hacerlo. Este tipo de controles es provisto por software de control de acceso.
- Software de control de acceso – permite que el administrador establezca reglas de seguridad para otorgar derechos de acceso para la protección de los recursos. Estos recursos pueden ser datos, programas, transacciones, computadoras o terminales individuales. El control de acceso puede indicarse por grupos de usuarios o clases de recursos, o a cualquier nivel de granularidad requerido para un recurso en particular.

Controles mínimos de software

- Revisión y aprobación - Debe existir un control de procedimiento de cambio de programas a realizar por alguien con conocimientos técnicos. Este control debe ser realizado por una persona diferente a quien realizó el cambio.
- Revisión y aprobación de plan de pruebas y resultados
- Respaldo y recuperación
- Historia y auditoría – debe existir documentación sobre los cambios realizados en el software: el cambio requerido, el trabajo realizado, los planes de prueba, los resultados de

prueba, las aciones correctivas, aprobaciones, quién realizó el trabajo, etc.
- Control de versión y configuración – se refiere a matener control sobre el software del que se obtuvo una copia para modificar, el que se está cargando a las bibliotecas de producción, etc.
- Pruebas periódicas - significa tomar un caso de prueba y periódicamente correr el sistema con datos conocidos que tienen resultados predecibles.
- Controles aleatorios – en el ambiente de producción
- Segregación de tareas - la idea es que ninguna persona tiene el control total sobre la modificación de programas y el proceso de validación, para evitar que alguien pueda cometer fraudes o dañar a la organización. Por ejemplo, alguien diferente a quien realizó la modificación debería pasarlo a producción.
- Software de control de acceso – en algunas aplicaciones puede tener un impacto económico negativo para la empresa que se haga público el código fuente. Por lo tanto debe protegerse de acceso no autorizado.
- Chequeo de virus

Definición de roles y responsabilidades

Para que esto sea efectivo debe haber un programa de entrenamiento.
No todos los roles que definamos son aplicables a cualquier esquema de clasificación de los datos, y puede que varios roles sean desempeñados por la misma persona.

- Propietario de la información – gerente del área de negocios responsable de esa información. Sus tareas pueden ser:
  - Asignar clasificación inicial de la información y periódicamente revisar que sigan cumpliendo con los requerimientos del negocio.
  - Asegurarse de la existencia de los controles de seguridad adecuados
  - Determinar requerimientos de seguridad, criterios de acceso, y requerimientos de respaldos
  - Realizar o delegar autoridad de aprobación para requerimientos de acceso
- Custodio de la información – en general es del área de TI, con responsabilidad de respaldos y recuperación de los datos
- Propietario de la aplicación – gerente de la unidad de negocios quien es responsable del desempeño de la unidad de negocios. Sus tareas puede incluir:
  - Administración de seguridad del día a día
  - Aprobación de requerimientos de acceso excepcionales
  - Acciones apropiadas por violaciones a la seguridad cuando es notificado por el administrador de seguridad
  - Revisión y aprobación de todos los cambios a la aplicación antes de pasarla al ambiente de producción
  - Verificación del estado de los derechos de acceso de los usuarios a la aplicación
- Jefe del usuario – es el supervisor directo de un empleado. Tiene k}la responsabilidad directa de todas las identificaciones de usuarios y la información que les pertenece. En caso de contratados o consultores, tiene la responsabilidad de su actividad y los activos de la empresa que estos utilicen. Su responsabilidad incluye:
  - Informar al administrador de la seguridad sobre un usuario que se va de la empresa, de

modo de revocar esos accesos y/o mantener la información inaccesible.
  - Informar al administrador de la seguridad sobre la transferencia de un usuario a otra área si involucra cambios en los derechos de acceso.
  - Reportar cualquier incidente o sospecha de incidente de seguridad
  - Recibir y distribuir contraseñas iniciales de nuevos usuarios
  - Educar empleados con respecto a políticas y procedimientos de seguridad
- Administrador de seguridad – esta persona establece los controles de seguridad, administra las identificaciones de usuario y derechos de acceso. Sus responsabilidades son:
  - Entender los diferentes ambientes de datos y el impacto de otorgar acceso a ellos
  - Asegurarse de que los requerimientos de acceso sean consistentes con las directivas de seguridad
  - Administrar los derechos de acceso de acuerdo a los criterios establecidos por los propietarios de la información
  - Crear y borrar identificaciones de usuario de acuerdo a las indicaciones del jefe de usuario, así como otorgar contraseñas a los usuarios creados.
  - Realizar seguimiento de reportes de violaciones de seguridad
- Analista de seguridad – es responsable de terminar la dirección de seguridad de datos (estrategia, procedimientos, guías) para asegurar que la información está protegida de acuerdo a su valor , riesgo de pérdida o compromiso, y facilidad de recuperación.
- Analista de control de cambios – es la persona encargada de revisar los requerimientos de cambios y analizar el impacto en las aplicaciones.

Clasificación de información y aplicaciones

Los propietarios de la información deben ser entrenados para saber cómo recolectar datos sobre su área de negocios, con un criterio orientado al manejo de la seguridad.
Luego de recolectar estos datos, deben clasificar la información, de acuerdo a los siguientes criterios:

- Información de auditoría
- Segregación de tareas requerida
- Requerimientos de criptografía
- Mecanismos de protección de datos
- Procesos de respaldo y recuperación
- Control de cambios
- Nivel de confidencialidad
- Requerimientos de retención de datos
- Ubicación de los documentos

Seguimiento

El departamento de auditoría interna debe liderar el esfuerzo de asegurar el cumplimiento de las políticas y establecer los procedimientos. Los propietarios de la información deberían realizar revisiones periódicas para asegurarse de que las categorías aún están vigentes, y además debe revisarse los controles asociados a cada categoría.
También deben realizarse revisiones periódicas de los permisos de acceso para asegurarse de que

aún cumplen con los requerimientos del trabajo.

Seguridad

Breve historia de la seguridad

La manera en que manejamos la seguridad de la información y de otros valores ha evolucionado con el correr del tiempo a medida que la sociedad y la tecnología han evolucionado también. Comprender esta evolución es importante para entender qué tanto necesitamos enfocarnos en la seguridad hoy en día.

Seguridad Física

En los primeros tiempos, todos los bienes era físicos.La informacón importante también era física, pues era grabada en pa piedra y más tarde, escrita en papel. En realidad, la mayoría de los líderes históricos no ponían información sensible o crítica en ninguna forma permanente. Tampoco la discutían públicamente, excepto con sus discípulos elegidos. Por lo tanto, la información era, y sigue siendo PODER. Tal vez esta era la forma más segura. Sun Tzu decía que “un secreto que es conocido por mpas de una persona ya no es un secreto.”
Para proteger lso bienes físicos, se usaba seguridad física como paredes, fosos, y guardias.
Si se transimitía la información, iba normalmente por un mensajero con un guardia. El peligro era puramente físico. No había forma de alcanzar la información sin tomarloa físicamente.
En la mayoría de los casos, el bien (dinero o información escrita) era robado. El propietario original era privado de su bien.

Seguridad en la comunicación

Desafortunadamente, la seguridad física tenía un defecto. Si se capturaba un mensaje en tránsito, la información
del mensaje caía en manos del enemigo. En los tiempo de Julio César se identificó este desperfecto y la solución fue seguridad en las comunicaciones. Julio César creó el Código César. Esto el permitía enviar mensajes que no podían ser interpretados si eran interceptados.
Este concepto continuó en la 2a. Guerra Mundial. Alemania usaba na máquina llamada Enigma, para encriptar mensajes que enviaba a unidades militares, y creyeron que era indestructible.
Si se hubiera usado apropiadamente seguramente hubiera sido bastante difícil, pero hubo algunos errores de los operadores y los aliados pudieron leer algunos mensajes (luego de utilizar una cantidad considerable de recursos para resolver el problema).
Las comunicaciones militares también usaban palabras claves en sus mensajes, para referirse a unidades y lugares.
Los japoneses usaban palabras claves para sus objetivos durante la guerra y esto hacía muy difíil entender sus mensajes aún cuando el código había sido quebrado.
Luego de la segunda guerra mundial, la unión Soviética usaba lo que llamaron “one-time pads”

para proteger la información transmitida por los espías. Esto no era más que bloques de papel con números alatorios en cada página. Cada página se usaba para uno u solo un mensaje. Este esquema de encriptación es inquebrantable se usa apropiadamente, pero comentieron el error de reutilizarlos, así que sus mensajes fueron descifrados.

Seguridad de Emisión

Aparte de los errores en su uso, los sistemas de encriptación son difíciles de quebrar.
De modo que se hicieron intentos de encontrar otros métodos para capturar información que era transmitida de forma encriptada. En los años 1950s, enontraron que se podía lograr el acceso a los mensajes revisando las señales electrónicas que iban por las líneas telefónicas.

Todos los sistemas electrónicos tienen emisiones electrónicas. Esto incluye los teletipos y los encriptadores que se usados para enviar los mensajes. El encriptador, toma el mensaje, lo encripta y lo envía por la línea telefónica. Las señales electrónicas que representaban en mensaje original, también estaban en la línea telefónica. Esto significaba que los mensajes se podían recuperar con algún buen equipo.
Esto hizo que EEUU creara un programa llamado TEMPEST. Este programa creaba emisiones eléctricas estándares para computadoras en ambientes muy sensibles. El objetivo era reducir emisiones que pudieran ser usadas para reunir información.

Seguridad de computadoras

La seguridad de comunicaciones y emisiones era suficiente cuando los mensajes eran transmitidos por teletipo. Entonces aparecieron en escenas las computadoras y la mayoría de la información de las organizaciones fue
migrada al formato electrónico. Con el tiempo, las computadoras se volvieron más fáciles de usar y más gente tuvo acceso a ellas con sesiones interactivas. la información de los sistemas se hizo accesible a cualquiera que tuviera acceso al sistema.
En los comienzos de los años 1970s, David Bell y Leonard La Padula desarrollaron un modelo para operaciones seguras de computadora. Este modelo se basaba en el concepto del gobierno de EEUU, de contar con varios niveles de información clasificada (no clasificada, confidencial, secreta, y super secreta) y varios niveles de
permisos. Así, si una persona (sujeto) tenía un nivel de permisos que dominaba (era mayor que) el nivel de clasificación de un archivo (objecto), esa persona podía acceder al archivo. En caso contrario, se negaba el acceso.
Este concepto de modelado condujo al Estándar 5200.28 del Depto. de Defensa de EEUU, el Trusted Computing System Evaluation Criteria (TCSEC, Libro Naranja) en 1983. El Libro Naranja define los sistemas computracionales de acuerdo a la siguiente escala:
D Protección Mínima o no ranqueada
C1 Protección de Seguridad Discrecional
C2 Protección de Acceso Controlado
B1 Protección de Seguridad Nominada
B2 Protección Estructurada
B3 Dominios de Seguridad

A1 Diseño Verificado

Para cada división, el Libro Naranja definió requerimientos funcionales y de aseguramiento. Los requerimientos de aseguramiento para las certificaciones más seguras tomaban un tiempo considerable y costaba mucho dinero. Esto resultó en pocos sistemas certificados por encima de C2 (en realidad, solo 1 sistema fue certificado como A1, el Honeywell SCOMP) y los que eran certificados era obsoletos para cuando habían completado el proceso.
Otro criterio intrntó separar la funcionalidad del aseguramiento. Estos esfuerzos incluyeron el Libro Verde Alemán de 1989, el Criterio Canadiense en 1990, the Information Technology Security Evaluation Criteria (ITSEC) en 1991, y el Federal Criteria en 1992. Todos ellos intentaban encontrar un método de certificación de sistemas computacionales seguros.
El ITSEC y el Federal Criteria fueron tan lejos hasta dejar el criterio de funcionalidad prácticamente indefinido.
El concepto era que los ambientes de aplicaciones comunes desarrollarían su propio perfil para funcionalidad de seguridad y niveles de aseguramiento. Estos perfiles serían usados entonces por alguna autoridad para certificar el cumplimiento de los sistemas computacionales
Al final, la tecnología de los sistemas de computadores evolucionó demasiado rápido para los programas de certificación. Nuevas versiones de sistemas operativos y hardware estaban siendo desarrollados y comercializados antes de que los sistemas más viejos pudieran ser certificados.

Seguridad de red

Otro problema relacionado con el criterio de evaluación de la seguridad de las computadoras era la falta de entendimiento de las redes. Cuando las computadoras participan de una red, nuevos problemas de seguridad aparecen, y los viejos problemas aparecen de forma diferente. Por ejemplo, tenemos comunicaciones pero las tenemos sobre LANs en vez de WANs. También tenemos mayor velocidad y muchas conexiones a un medio común. Los encriptadores dedicados podrían no ser útlies en este entorno. También tenemos emisiones de los cables de cobre que están en el edificio. Finalmente, tenemos acceso de los usuarios desde muchos sistemas diferentes sin el control de una única máquina central.
El Libro Naranja no rataba este tema de computadoras conectadas en red. En realidad, accesso de red podía invalidar la certificación. La respuesta a esto fue la Trusted Network Interpretation of the TCSEC (TNI, o el Libro Rojo) en 1987. El Libro Rojo tomó todos los requerimientos del Libro Naranja, e intentó tratar el tema de ambientes de red. Desafortunadamente, también encadenó funcionalidad con aseguramiento. Pocos sistemas fueron evaluados con esta certificación, y ninguno tuvo éxito comercial.

Seguridad de la Información

En la realidad, para lograr un buen nivel de seguriad, debe emplearse unamezcla de todas las soluciones. Buena seguridad física es necesaria para proteger los bienes físicos como registros en papel y los propios sistemas. Seguridad de las comunicaciones es necesaria para proteger la información en tránsito. Seguridad de las emisiones puede ser necesaria si el enemigo tiene suficientes recursos como para leer las emisiones de nuestras computadoras. Y seguridad en la red es necesaria para controlar el acceso a nuestra red local.
Todos estos conceptos proveen seguridad de la información.

Siguen habiendo dificultades para demostrar que algo es seguro, además, la tecnología sigue avanzando demasiado rápido.
Lo importante entonces, es mantener buenas prácticas de seguridad y controlar periódicamente.
La seguridad de la información en las empresas de hoy es *"una bien informada convicción de que los riesgos y los controles están balanceados"* - Jim Anderson, Inovant (2002)

Una breve reseña histórica

1960s

- Department of Defense's Advanced Research Procurement Agency (ARPA) comenzó a analizar la viabilidad de un sistema de comunicaciones de red redundantes diseñado para soportar necesidades de intercambio de información militar.

1970s-1980s:

- ARPANET creción epopularidad y uso,y también su potencial uso malicioso.
- 1973: Robert M. Metcalfe, indicó que había problemas de seguridad fundamentales en ARPANET.
- Sitios de usuarios remotos individuales no tenían suficientes controles y garantías para proteger sus datos contra acceso no autorizado de usuarios remotos.
- No habían procedimientos de seguridad para conexiones dial-up a ARPANET.
- No existía idenificación y autorización de usuarios a los sistemas.
- Los números de teléfono se distribuian y publicitaban abiertamente en los muros de la calle, dándole a los hackers acceso fácil a ARPANET.

1990s

- Al final del siglo XX, como las redes de computadores e volvieron más comunes, también creció la necesidad deinterconectarlas.
- Esto hizo crecer internet, la primera manifestación de una red global de redes.
- En las primeras implementaciones de internet, la seguridad tenía un papel menor, o ninguno.
- A medida que los requerimientros de redes de computadores se volvió más dominante, la capacidad de asegurar físicamente la computadora ya no fue suficiente, y la información almacenada estuvo más expuesta.

El presente

- Hoy en día, Internet ha traído millones de redes de cmputadoras inseguras comunicándose con los otros.
- Nuestra capacidad de asegurar la información almacenada está limitada por la seguridad en cada computadora a la que está conectada.

Seguridad y Administración de Sistemas de Información

Introducción

Hablar de seguridad para los sistemas informáticos significa hablar de un proceso de concientización. Hay varios factores que han acelerado este proceso, y captado más atención sobre el tema:

- El problema del año 2000: ha hecho que los altos directivos o gerentes hayan tomado conciencia de la importancia y el valor de la información y el soporte de los centros de cómputo
- La llegada al ámbito empresarial de la computación distribuida: con la tecnología cliente/servidor se facilita el acceso a las bases de datos no solo a los empleados sino que también a los clientes externos a la organización.
- La tecnología de Internet: hace necesario implantar soluciones que impidan el acceso a las bases de datos, y permitan el acceso sólo a la información permitida.

A medida que la tecnología evoluciona, la protección de los recursos se vuelve cada vez más compleja. A pesar de ello, la seguridad es un tema predominantemente organizacional, y por lo tanto es importante establecer y hacer que se cumplan políticas y estándares de seguridad para una Administración exitosa de un Programa de Seguridad de la Información.

Veamos algunos datos:

1990-2002

Año	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002
Incidentes	6	132	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	52,658	82,094

Total de incidentes reportados (1988-2002): **182,463**
Notar que un incidene puede involucrar uno o varios sitios.

1995-2002

Año	1995	1996	1997	1998	1999*	2000	2001	2002
Vulnerabilidades	171	345	311	262	417	1,090	2,437	4,129

Total de vulnerabildades reportadas (1995-2002): **9,162**
(fuente: www.cert.org)

Lo importante en destacar no es la cantidad absoluta, sino la tendencia creciente de incidentes, y de “agujeros” en las aplicaciones corrientes, que pueden ser explotadas maliciosamente. Por esto, resulta claro la necesidad de destinar recursos y tiempo a la protección de la información.
Sin embargo, para que un sistema de seguridad sea viable, debe cumplir los siguientes requisitos:

- Eficiente
- Simple
- Standard
- No caro

Para adaptarse a la apertura, las empresas en general lo han hecho paulatinamente, integrando "pedazos" de soluciones de seguridad, principalmente cuando conviven en la organización diferentes plataformas y sistemas operativos. Sin embargo, en muchos casos aún no hay un nivel de integración de la seguridad, sino que se ven como subproyectos. Pero cuando se incorporan tecnologías como por ejemplo, a un mainframe o mini se le integra cliente/servidor, el primero pasa a funcionar como un disco para un PC, por lo que estos últimos deben estar protegidos adecuadamente. Además se pueden almacenar virus en el mini, que aunque no lo dañen, pueden contagiar a otros equipos.

En los años '90 comenzó a expandirse la cultura de seguridad de los sistemas. La seguridad debe verse como un nivel de continuidad y no como métodos alternativos de servicio. Si bien uno puede elegir una plataforma considerada como muy segura (caso AS/400), con la apertura a otras plataformas que invariablemente se requiere hoy en día, surge la necesidad de implantar una metodología standard que ayude a brindar un nivel de seguridad óptimo y compartido.

Objetivo de la seguridad

Garantizar la disponibilidad, confidencialidad e integridad de la información relevante para el funcionamiento de la empresa.

Amenazas y vulnerabilidad

Que afecten la disponibilidad:
- Desastres naturales, o artificiales ajenos a la empresa
- Planes de contingencia de TI inadecuados
- Planes de continuidad del negocio inadecuados
- Pobre desempeño de sistemas (degradado)

Que afecten la confidencialidad:
- Gente ajena a la empresa que consiga acceder a documentos e impresos con información sensible
- Exposición, por parte de los empleados, de información sensible a gente ajena a la empresa
- Acceso no autorizado a datos por parte de los empleados o terceros
- Interceptación de líneas de comunicación

Que afecten la integridad:
- Errores de entrada
- Errores de programas
- Errores de operación
- Manipulación o supresión de documentos de entrada
- Uso no autorizado de facilidades de transacciones
- Modificación no autorizada de archivos
- Manipulación de colas de trabajo

- Problemas de integridad con sistemas de alimentación (interfaces)

Principios

- Contabilidad: medible. Toda acción debe ser rastreable
- Conocimiento: debe darse amplia difusión sobre los posibles riesgos y las normas de seguridad
- Multidisciplinariedad: no solo involucra al área de TI y sus funcionarios, sino que se debe tomar en cuenta todas las funciones críticas.
- Proporcionalidad: debe haber una relación razonable costo-efectividad.
- Integración: debe estar coordinada con las otras áreas funcionales de la empresa. Debe haber una política integradora.
- Tiempo: debe darse una respuesta oportuna, definiéndose el tiempo máximo para que esta respuesta sea efectiva.
- Factores sociales: éticos.

Etapas

- ***Definición de compromiso***: esto significa desarrollar políticas, difundirlas y actualizarlas. Para ello, la alta gerencia debe promover y fijar los lineamientos para adoptar normas de seguridad.
- ***Organización de Recursos Humanos***: deben designarse las personas involucradas, y el papel de cada una de ellas (roles y responsabilidades). En último término, toda la compañía está involucrada, con mayor o menor grado de responsabilidad y compromiso.
- ***Asignación de valor a los recursos de información***: asignar importancia relativa a cada recurso. Las tareas relacionadas son: identificar los recursos de valor para el negocio, clasificar la información de acuerdo a su importancia, realizar análisis de riesgo para sistemas críticos para el negocio.
- ***Protección de los recursos de información***: esto significa definir el diseño del marco de trabajo. Debe asegurarse de que las medidas de seguridad adecuadas están vigentes. Para ello es necesario definir procedimientos, prácticas, estándares y medidas:
    - Procedimiento para las adquisiciones
    - Procedimiento para el pasaje de aplicaciones a producción
    - Procedimiento de respaldos
    - Procedimientos de operación
    - Asignación de responsabilidades
    - Procedimiento de autorización de acceso a la información
    - Procedimiento para la documentación de aplicaciones
    - Procedimiento para la implementación de aplicaciones
- ***Promoción de las mejoras***: Es necesario también promover las mejoras, asegurándose que las unidades de negocio que deseen actualizar la seguridad de la información tengan acceso a los expertos y los servicios que necesitan. Las tareas relacionadas son: definir terminología, estándares y guías, llevar a cabo proyectos de seguridad, operar un programa de concientización, y un programa de desarrollo de habilidades, proveer un servicio de análisis

de riesgo, proveer un servicio de aseguramiento del cumplimiento, implementar las medidas de mejora, estar al dái con los nuevos desarrollos

- ***Establecimiento de reglas de monitoreo***: para detectar áreas expuestas, o no cubiertas por las normas vigentes, o circunstancias especiales que creen un vacío normativo. Para esto se debe definir indicadores clave de desempeño, recoger datos de desempeño y planes, elaborar reportes y revisar los resultados a alto nivel de gerencia.
- ***Difusión:***
    - Conocimiento: todos los integrantes de la compañía deben saber que existen normas de seguridad, y procedimientos a seguir para salvaguardar la información
    - Entrenamiento: para operar los sistemas de información en forma segura
    - Educación: en las reglas y prácticas

Políticas de Seguridad

¿Qué son las políticas de seguridad?

Intuitivamente, se refieren a las normas y procedimientos definidos para asegurar la disponibilidad e integridad de la información y recursos de una organización.
El término "política de seguridad" en el contexto de la computación tiene varios significados. En primer lugar, política se refiere a directivas de la alta gerencia para crear un programa de seguridad de computadoras, establecer sus metas, y asignar responsabilidades. Política también es el conjunto de reglas de seguridad para sistemas particulares. En tercer lugar, política puede referirse a asuntos totalmente diferentes, tales como las decisiones gerenciales estableciendo la política de privacidad de correo electrónico de una organización.

¿Para qué sirve una política de seguridad?

- Para ayudar a prevenir incidentes
- Para definir responsabilidades y expectativas:
  - cumplir los requerimientos de protección de la tecnología y activos de la información
  - toma de conciencia por parte de los usuarios
  - uso aceptable de usuarios regulares y con privilegios especiales
- Para proveer una guía cuando ocurre un incidente
  - manejar incidentes de manera más efectiva
  - manejar incidentes de manera más eficiente
  - reducir el impacto de los incidentes

Tipos de políticas

Las organizaciones deberían tener 3 tipos de políticas:

1. Política de programa: una política de programa de una organización debe:
    - crear y definir un programa de seguridad de computación: debe ser claro en cuanto a qué recursos cubre (hardware, software, personal, información)
    - establecer direcciones estratégicas de la organización: puede incluir definición de metas

del programa, como por ejemplo, reducción de errores.
   - asignar responsabilidades: para la implementación del programa
   - referirse al cumplimiento de la política: requerimientos para establecer el plan y también qué penalizaciones se aplicarán a quienes no cumplan la política.
2. Política de asuntos específicos: una política de este tipo debe:
   - Tratar áreas específicas de relevancia para la organización, como por ejemplo, conectividad a internet o privacidad de correo electrónico.
   - Ser actualizada con frecuencia, a medida que aparecen cambios en la tecnología utilizada.
   - Contener una declaración del asunto: la posición de la organización, aplicabilidad, roles y responsabilidades, cumplimiento y punto de contacto.
3. Política de sistemas específicos: una política de este tipo debe:
   - Enfocarse en decisiones: las decisiones tomadas por la gerencia para proteger un sistema en particular, tales como definir hasta dónde se registrará las acciones de los individuos.
   - Debe realizarse basada en un análisis técnico
   - Variar de un sistema a otro: esto ocurre porque cada sistema necesita objetivos de seguridad definidos basados en los requerimientos operacionales, ambiente y aceptación del riesgo por parte de la gerencia.
   - Ser expresadas como reglas: quién (por categoría de trabajo, ubicación dentro de la organización o nombre) puede hacer qué (modificar, borrar) a qué clase específica de registros de datos y en qué circunstancias.

Las políticas de seguridad son un medio para alcanzar las metas propuestas por una organización y no se deben interpretar como un fin en sí mismas.

Condiciones de las políticas

Los tres tipos de política deben ser:
- Realistas: que sea posible implementarlas
- complementadas: como se definen en un nivel muy amplio, es necesario desarrollar estándares, guías y procedimientos que ofrezcan a los usuarios, gerentes y otros un enfoque más claro de la implementación de la política y cómo llegar a las metas de la organización. Estos estándares, guías y procedimientos deben ser difundidos dentro de la organización vía manuales, regulaciones, etc.
- visibles: el hecho de que sea comunicada en toda la organización ayuda a implementarla.
- apoyadas por la gerencia: sin su apoyo la política no es efectiva. Si en cambio, tienen el apoyo de la gerencia se pueden hacer cumplir.
- Consistentes: otras directivas, leyes, cultura organizacional, guías, procedimientos y la misión de la organización deben tenerse en cuenta a la hora de formular implementar una política.
- Actualizadas: deben acompasarse a los cambios tecnológicos y organizacionales

¿Quiénes definen la política de seguridad y quiénes están involucrados?

Para no perder de vista los objetivos de la organización, deben ser definidas por los gerentes y

mandos altos de la organización, pero para asegurar la factibilidad técnica deben ser definidas en conjunto con el área de soporte técnico.
Para que una política de seguridad sea consistente debe involucrar a todos los integrantes de una organización.

Análisis de riesgos y amenazas

Una de las principales razones para crear una política de seguridad es asegurar que los esfuerzos puestos en la seguridad llevan a beneficios efectivos desde el punto de vista de la relación costo-beneficio.
El análisis de riesgos involucra identificar:

- qué se debe proteger
- de qué se debe proteger
- cómo se debe proteger

Para cada bien identificado como objeto a proteger, los objetivos básicos de seguridad son:

- Disponibilidad
- Confidencialidad
- Integridad

Las amenazas identificadas deben ser analizadas teniendo en cuenta cómo pueden afectar estos objetivos.

¿Qué se debe proteger?

1) Hardware
2) Software
3) Datos (durante la ejecución, almacenado on-line, u off-line, backups, logs de auditoría, bases de datos, o datos en tránsito sobre los medios de comunicación).
4) Personas
5) Documentación (de programas, hardware, sistemas, procedimientos administrativos locales)
6) Suministros

Estos bienes deben ser valorizados mediante un análisis costo-beneficio del esfuerzo invertido en protegerlos.

¿De qué se debe proteger?

Acceso no autorizado

Se refiere a intentos de acceder a recursos computacionales para los cuales no se tiene autorización previa. Una de las formas de acceso no autorizado más peligrosas, es el uso de la cuenta de otro usuario para ganar acceso a los sistemas. Esto puede ser la puerta para otras

amenazas a la seguridad, especialmente si dicho acceso se hace con privilegios de administrador. En este caso sería posible que el intruso cambiara la configuración de los sistemas, por ejemplo, poniendo un script de inicio que impida el normal funcionamiento del sistema.

Divulgación de información

Es necesario establecer el valor de la información almacenada en el sistema. La divulgación de un archivo de contraseñas puede permitir futuros accesos no autorizados. La filtración de información estratégica de negocios puede dar a un competidor una ventaja desleal.

Denegación de servicios

Se refiere a la no disponibilidad de los servicios ofrecidos por la computadora, por lo que se produce una pérdida en la productividad.
Es necesario identificar aquellos servicios que se consideran esenciales y cómo se vería afectada la red en caso de no estar disponibles.

Pérdida o corrupción de información

Es necesario evaluar los riesgos de contar con información incorrecta o alterada en forma voluntaria, o aún involuntaria, por usuarios del sistema o agresores externos. Muchas decisiones importantes se basan en el grado de certidumbre de la información que manejamos.

¿Qué hacer cuando se detectan violaciones a la seguridad?

Hay dos estrategias opuestas a seguir en caso que se detecte una violación a la seguridad:

Proteger y seguir

Esta estrategia tiene como objetivo primario la protección y preservación de las facilidades de la red y proveer a sus usuarios de los servicios habituales tan rápidamente como sea posible. Se llevan a cabo acciones para interferir con la actividad de los intrusos, prevenir futuros accesos y comenzar de inmediato la evaluación de los daños recibidos y la recuperación. Este tipo de procedimientos puede incluir “bajar” los sistemas, o cancelar todo acceso a la red.
La desventaja de esta estrategia, es que, a menos que el intruso sea identificado directamente, podría volver a ingresar al sistema por un camino diferente, o atacar otro sitio.

¿Cuándo adoptar esta estrategia?

- Los sistemas no están bien protegidos
- La intrusión continuada puede redundar en grandes daños económicos
- Los usuarios no son elaborados y su trabajo es vulnerable
- El sitio es vulnerable a acciones legales por parte de los usuarios que se vean afectados por el incidente

Búsqueda y captura

El objetivo principal de esta estrategia es permitir a los intrusos continuar con sus actividades en el sistema, hasta tanto no sean identificados los responsables. La captura no es la única acción posible si el culpable es identificado; si, por ejemplo, es un empleado, puede ser separado de su cargo o pueden tomarse acciones disciplinarias.
La desventaja de esta estrategia es que se está exponiendo a la organización a recibir daños más severos, en tanto el intruso puede seguir sus actividades libremente.

¿Cuándo adoptar esta estrategia?

- Los sistemas están bien protegidos
- Se dispone de buenos respaldos
- El riesgo a los bienes es secundario comparado con el problema causado por la presente y futuras violaciones a la seguridad
- El ataque se produce con gran frecuencia e intensidad
- Se puede controlar el acceso de los intrusos
- El equipo de trabajo tiene la capacidad y los conocimientos suficientes sobre los sistemas operativos, las herramientas y los sistemas como para permitir identificar a los intrusos
- Las herramientas de monitoreo son eficientes como para permitir el seguimiento de las actividades y la identificación del o de los intrusos
- Se está dispuesto a correr el riesgo legal por posibles daños causados a los usuarios de los sistemas

Procedimientos de Seguridad

Procedimientos para prevenir brechas en la seguridad

La política de seguridad define qué partes de nuestro sistema necesitan ser protegidas. Los procedimientos indican cuáles son los pasos a seguir para ponerla en práctica.
Es común comenzar a crear procedimientos de seguridad, decidiendo los diferentes mecanismos primero: contraseñas, smartcards, etc. Comenzar con la política de seguridad y los riesgos que ella subraya, nos asegura que los procedimientos proveen el nivel adecuado de protección para todos los riesgos.

Estructura común para estándares, guías y controles

- Nivel básico: documentación de procedimientos, de sistemas, acuerdo de nivel de servicio, planeación de la capacidad, respaldos, protección contra virus
- Protección física: falla eléctrica, fuego, equipos de emergencia y procedimientos
- Personal: descripción de tareas, acuerdo de confidencialidad, separación de tareas, contratados
- Control de accesos: identificación, autorización, control de usuarios externos, control de privilegios especiales
- Telecomunicaciones: confidencialidad de mensajes, enrutamiento de mensajes, acuerdos con terceros
- Registro de eventos (log) y seguimiento
- Planes de continuidad

- Adquisición de sistemas: compras centralizadas, proceso de selección, proveedores y productos aprobados
- Construcción de seguridad en los sistemas: procesos y ambiente de desarrollo, definición de requerimientos, controles de verificación y entrega
- Cambios en los sistemas operacionales y facilidades: definición de alcance de los cambios, proceso de administración del cambio, manejo de emergencia, evitar la obsolescencia, consistencia

Problemas de seguridad

- **Puntos de acceso**: Los puntos de acceso son típicamente los usados por usuarios no autorizados. El tener varios puntos de acceso incrementa ese riesgo. Las líneas discadas, dependiendo de su configuración, pueden proveer acceso a un sistema aislado o si están conectadas a un servidor, pueden dar acceso a toda la red.

- **Sistemas mal configurados**: Este problema es responsable de un gran porcentaje de los "agujeros" de seguridad. La creciente complejidad de los sistemas operativos y el software asociado hace difícil entender como funcionan los sistemas. Por otra parte, a menudo, los administradores de los sistemas son no especialistas elegidos entre el personal de la organización en el momento de implantarse los sistemas.

- **Errores de software**: Los sistemas nunca son 100% libres de errores. Los errores conocidos públicamente de los sistemas operativos son métodos comunes de acceso no autorizado. Parte de la solución de este problema es estar alerta de los errores detectados y actualizar el software ya sea con las nuevas versiones o con los parches liberados. Cuando se detecta un problema, este debe ser reportado al fabricante del sistema, como forma de ser corregido en las versiones posteriores.

- **Amenazas internas**: Los miembros de la organización pueden ser una amenaza considerable a la seguridad de los sistemas. Estos a menudo tienen acceso directo a las computadoras y recursos de red del sistema. El acceso a una LAN provee la capacidad de ver información posiblemente sensible viajando a través de la red.

- **Seguridad física:** Si un sistema no es físicamente seguro, todos los esfuerzos aplicados en la seguridad serán inútiles. Si un intruso tiene acceso físico a una máquina, puede detenerla y cambiarla a un modo privilegiado, reemplazar o alterar discos, plantar virus, o cualquier otra acción que perjudique el normal funcionamiento de la red. Los servidores importantes, enlaces de comunicaciones críticos y otras máquinas claves deben estar en áreas físicamente seguras. Algunos sistemas de seguridad, como Kerberos, requieren que la máquina que los implemente sea físicamente segura. Si algunas máquinas no se pueden asegurar físicamente, se debe tener especial cuidado en la confianza puesta en esas máquinas y la información que manejan.

Procedimientos para detectar actividad no autorizada

El procedimiento más simple usado para detectar la mayoría de los usos no autorizados, es el

monitoreo del uso de los sistemas. Este puede ser hecho por los administradores de los sistemas o por software creado con tal función. Monitorear un sistema implica mirar en diferentes partes del sistema, buscando algo inusual. Debe hacerse regularmente para que sea efectivo, aunque debe tenerse en cuenta el factor sorpresa, es decir no es demasiado efectivo efectuarlo siempre el mismo día o a las mismas horas.
Existen varias herramientas y métodos disponibles:

- **Logging**: La mayoría de los sistemas guardan gran cantidad de información en los archivos de registro de actividad (logs). Es útil registrar dichos archivos buscando por ejemplo, entradas a los sistemas en horas inusuales, reiterados intentos fallidos de conexión por un mismo usuario, o mensajes de error extraños, como intentos de acceso a información protegida por usuarios no autorizados.

- **Software de monitoreo**: Se pueden utilizar las herramientas facilitadas por los sistemas operativos (por ejemplo los comandos *ls* y *find* de UNIX y chequear contra la lista de usuarios). Otra opción son las herramientas que, aunque no son de uso específico para el control de la seguridad, pueden ser utilizadas para el control de los sistemas desde ese punto de vista. Un ejemplo de ello son los monitores de red, que pueden usarse para detectar conexiones de red desde sitios desconocidos.

- **Detección de situaciones anormales:** Hay indicaciones que nos permiten sospechar la ocurrencia de incidentes:

    - Caída de los sistemas sin explicación
    - Nuevas cuentas de usuario desconocidas
    - Nuevos archivos, usualmente con nombres extraños
    - Discrepancias en los archivos de log, como desaparición o modificaciones en el tamaño.
    - Cambios en los tamaños de archivos o en fechas
    - Intentos de escritura en archivos del sistema
    - Modificación o borrado de datos
    - Denegación de servicio
    - Bajo rendimiento sin explicación
    - Situaciones extrañas
    - Actividad sospechosa (por ejemplo un usuario que accede a un archivo tras otro en un directorio con información sensible)

Tipos de procedimientos de seguridad

Auditorías de seguridad de sistemas

La auditoría implica la revisión y análisis de todas las políticas que conciernen a la seguridad del sistema, así como los mecanismos que las implementan.

Las auditorías detalladas deben ser realizadas sobre una base periódica prefijada, por ejemplo una vez al año, o a intervalos que se consideren necesarios. Dichas revisiones detalladas son una

forma de verificar si las políticas y procedimientos son efectivos. Por otro lado, las revisiones representan un importante consumo de tiempo, a la vez que una interrupción a las tareas normales. Es importante sopesar los beneficios de las revisiones contra la posible pérdida de tiempo que ocasionan.

Si se decide no usar auditorías detalladas prefijadas para examinar la totalidad de los procedimientos de seguridad al mismo tiempo, es importante chequear los procedimientos individuales frecuentemente.

Es importante verificar todos los aspectos de la política de seguridad, tanto los manuales como los automáticos, con particular énfasis en los mecanismos automáticos utilizados.

Se debe tener en cuenta que hay un límite razonable hasta donde se deben desarrollar las pruebas. El propósito de realizar dichas pruebas es lograr un nivel aceptable de certeza que la política de seguridad está correctamente implantada y que los controles impuestos son adecuados, y no que el sistema de seguridad es infalible.

Objetivos de la auditoría de LAN

- Estándares de la LAN: La gerencia debe proveer estándares para la operación efectiva y eficiente de los recursos.
- Seguridad de los datos: Asegurar que se han implementado controles efectivos para la seguridad de los archivos de datos y las librerías de programas.
- Administración y operación de los sistemas: Verificar que existen procedimientos y controles que aseguren que el sistema funciona en forma efectiva y eficiente en todas las fases de operaciones y mantenimiento en orden de proveer la máxima disponibilidad y rendimiento del sistema.
- Controles a los Sistemas y programas: Verificar que se ejerce un control adecuado sobre la instalación, mantenimiento y uso del software en uso en la red, tanto adquirido como desarrollado por internos.
- Ambiente y seguridad física: Asegurar que se utilizan procedimientos y equipamiento para proveer adecuada seguridad física para el equipamiento informático contra robo, vandalismo, fuego, etc.
- Plan de Contingencia: Asegurar que existe un plan adecuado para la recuperación en tiempo y forma de las operaciones de procesamiento luego de alguna forma de interrupción.
- Seguridad de comunicaciones: Asegurar que la gerencia ha instituido políticas y procedimientos que protegerán datos sensibles de ser modificados, interceptados o desprotegidos en la red.
- Entrenamiento y Educación de los Usuarios: Asegurar que los operadores, equipo de trabajo y usuarios del sistema, son adecuadamente entrenados en uso efectivo y eficiente de los recursos del sistema.

Administración de cuentas

Los procedimientos para la administración de las cuentas de usuario son importantes para prevenir acceso no autorizado a los sistemas. Es necesario decidir:

- ¿Quién debe tener una cuenta en el sistema?
- ¿Cuánto tiempo se puede tener una cuenta en el sistema sin que la solicitud sea renovada?
- ¿Cómo se eliminan las cuentas viejas del sistema?

Las respuestas a dichas preguntas deben estar descriptas explícitamente en la política de seguridad. Además de decidir quién puede usar el sistema, puede ser importante decidir para qué puede ser usado (por ejemplo si se permite el uso personal).

Es importante definir procedimientos de administración de cuentas adecuados tanto para los administradores como para los usuarios. Típicamente, los administradores serán responsables por la creación y eliminación de cuentas de usuario y el mantenimiento general de los sistemas y/o las redes. Por otra parte, la administración de las cuentas en responsabilidad de los usuarios, en el sentido que deben observar la existencia de mensajes y eventos que indiquen una violación a la política de seguridad y hacer un uso responsable de las cuentas. Por ejemplo, un mensaje de bienvenida que indique la fecha y hora del último ingreso al sistema o a la red deberá ser reportado si indica una fecha de ingreso no reconocida por el usuario.

Administración de contraseñas

La política de administración de contraseñas puede ser importante si se quiere reforzar las contraseñas seguras. Estos procedimientos pueden variar desde preguntar o forzar a los usuarios a cambiar sus contraseñas ocasionalmente hasta tratar de quebrar las contraseñas de los usuarios y entonces informar a estos lo fácil que esto resultó.
Mas allá de las políticas, los procedimientos de administración de contraseñas deben ser establecidos cuidadosamente. La elección de la contraseña inicial es crítica. En algunos casos los usuarios pueden no ingresar nunca a las cuentas, por lo tanto la contraseña inicial no debe ser fácilmente adivinable.

Estas son algunas preguntas útiles a la hora de definir políticas de administración de contraseñas:

- Existe segregación de roles entre la función de administración de LAN y administrador de seguridad
- Determinar que todos los usuarios deben ingresar una identificación de usuario y una contraseña para acceder a la LAN.

- Las contraseñas se muestran de forma ilegible
- Se encriptan las contraseñas en la terminal antes de ser enviadas al servidor para verificar
- El sistema fuerza al usuario a cambiar las contraseñas periódicamente.
- El sistema previene la reutilización de las contraseñas; se previene a los usuarios el peligro de cambiar a contraseñas previas
- Se fuerza a los nuevos usuarios a entrar una contraseña en su primer ingreso al sistema.
- Se exige el uso de un largo mínimo de contraseña.
- Se guardan las contraseñas como texto sin encriptar en algún lugar del sistema.
- Se desactivan las cuentas de usuario después de un tiempo de inactividad.
- Se permiten contraseñas de grupo.
- Los empleados firman que conocen la política de la organización frente a la divulgación de importación confidencial protegida por contraseñas.
- Se instruye a los usuarios sobre las políticas para establecer las contraseñas.

- Se restringe el uso de las cuentas a los días y horas de trabajo.
- Se deshabilitan las cuentas de usuarios después de varios intentos fallidos de ingreso.

Administración de configuración del sistema

Ya que se espera que la mayoría de los programas al nivel de sistema operativo ayuden a reforzar la política de seguridad, es necesario tener un grado de certeza razonable de que estos están correctamente configurados. Esto significa que no se debería permitir que las aplicaciones de nivel de sistema operativo sean cambiadas arbitrariamente. Los procedimientos deben establecer quién está autorizado a hacer cambios a los sistemas, en qué circunstancias, y cómo se deben documentar dichos cambios.
También es deseable aplicar la administración de configuración a la configuración física del equipamiento, manteniendo configuraciones válidas y actualizadas.

Configuraciones especiales (no estándar)

Puede ser útil tener una configuración algo diferente a lo habitual, para dificultar los ataques "estándares" usados por los hackers. Las partes no estándar de la configuración pueden incluir algoritmos de criptografía de las contraseñas diferentes, localizaciones de los archivos de configuración diferentes, y comandos del sistema re-escritos o limitados.
Sin embargo, las configuraciones no estándar tienen sus desventajas, como por ejemplo, que es más difícil el mantenimiento del software ya que se requiere documentación extra, y rehacer los cambios después de cada actualización de los sistemas operativos y generalmente, la presencia de personal con claro conocimiento de los cambios.

Por lo tanto, las configuraciones no estándar generalmente sólo son usadas en ambiente con un "firewall" instalado. El firewall es modificado en formas no estándar dado que es propenso a sufrir ataques, mientras que las configuraciones de los sistemas detrás del firewall se mantienen en su forma estándar.

Seguridad en Redes

¿Qué es una red de computadoras?

Una red de computadoras es un sistema de computadoras interconectadas.

¿Para qué sirven y por qué usarlas?

A lo largo del tiempo los sistemas de información han ido almacenando grandes cantidades de datos, creando una necesidad cada vez mayor de acceso a ellos. Además, han bajado mucho los costos de hardware, lo que ha hecho posible la proliferación de las redes de computadoras como alternativa económica y flexible a los sistemas centralizados. La flexibilidad que aportan las redes de computadoras al acceso a la información radica en la capacidad de disponer de múltiples fuentes alternativas de información y de un mejor aprovechamiento de los recursos,

como así también la posibilidad de independizar a los usuarios del lugar físico que ocupan.

También ha crecido el uso de redes con arquitecturas de tipo cliente-servidor, por la buena relación costo/beneficio: es más fácil hacer una adaptación a las necesidades crecientes en forma incremental en una red de computadoras con una estructura cliente-servidor que en un sistema basado en una gran computadora central que debe actualizarse.

Tipos de ataques a la seguridad

Los ataques a la seguridad en las comunicaciones se dividen en:

- **Pasivos**: Los ataques pasivos son la *escucha y divulgación de la información* y el *análisis de tráfico.* Esto no implica que se conozca el contenido de la información que fluye en una comunicación, pero el conocimiento de ese flujo, puede ser información útil.
- **Activos**:

  1 – *Enmascaramiento:* suplantación de un ente autorizado para acceder a información o recursos.
  2 – *Modificación:* incluye la posible destrucción y creación no autorizada de datos o recursos.
  3 – *Interrupción:* supone el impedir a entes autorizados su acceso a la información o recursos a los que tienen derecho de acceso.

Una visión general de los tipos de ataques

Trojan horses	*Fraud networks*	*Fictitious people*	*Infrastructure observation*	*e-mail overflow*
Time bombs	*Get a job*	*Protection limit poke*	*Infrastructure interference*	*Human engineering*
Bribes	*Dumpster diving*	*Sympathetic vibration*	*Password guessing*	*Packet insertion*
Data diddling	*Computer viruses*	*Invalid values on calls*	*Van Eck bugging*	*Packet watching*
Login spoofing	*Data diddling*	*Wiretapping*	*Combined attacks*	*e-mail spoofing*
Scanning	*Dumpster diving*	*Eavesdropping*	*Denial-of-service*	*Harassment*
Masquerading	*Software piracy*	*Data copying*	*Degradation of service*	*Traffic analysis*
Trap doors	*Covert channels*	*Viruses and worms*	*Session hijacking*	*Timing attacks*
Tunneling	*Trojan horses*	*IP spoofing*	*Logic bombs*	*Salamis*
Password sniffing	*Excess privileges*			

(fuente: www.cert.org)

¿Cómo defenderse de estos ataques?

- Minimizar la probabilidad de intromisión con la implantación de elementos de protección.
- Detectar cualquier intrusión lo antes posible
- Identificar la información objeto del ataque y su estado para recuperarla tras el ataque.

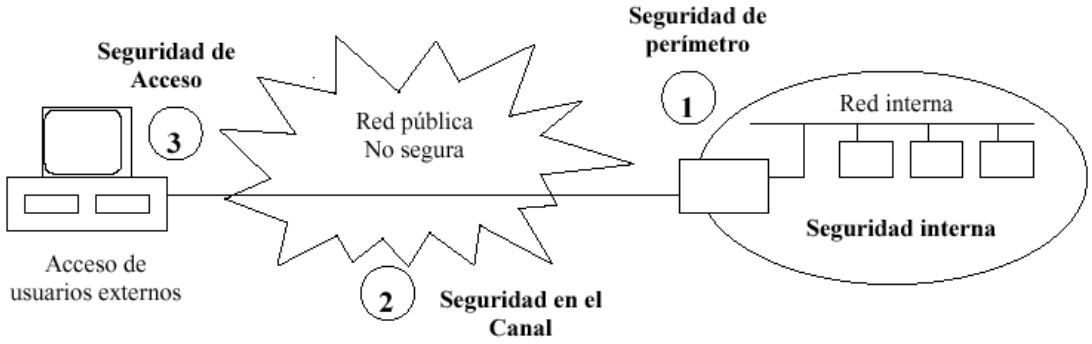
Sería interminable enumerar las posibles formas de ataque que puede sufrir una computadora conectada a una red de comunicaciones, bien por intervención física sobre los mismos o vía software. Las medidas de prevención son múltiples también, desde la vigilancia física del sistema, hasta el registro de los eventos que se producen en el sistema y la vigilancia de las modificaciones en aquellos archivos o procesos que son críticos para la seguridad del mismo.

Todo ello involucra la responsabilidad tanto de los usuarios como del administrador del sistema encargado de establecer las políticas de cuentas de usuario adecuadas.

Las tres áreas de la seguridad

Actualmente, cuando las empresas disponen ya de sus propias redes internas a las que dan acceso a usuarios desde el exterior, los problemas de seguridad se plantean en tres áreas principales:

1. **La seguridad de perímetro:** protección frente a ataques externos, generalmente basada en firewalls.
2. **La seguridad en el canal:** donde hay que proteger los datos frente a escuchas mediante ***criptografía.***
3. **La seguridad de acceso:** donde se contemplan tres aspectos, la *identificación* del usuario, la *autorización* del acceso y la *auditoría* de las operaciones realizadas por el usuario.



Sin embargo, a veces se olvida la **seguridad interna** ya que el problema de seguridad puede aparecer dentro de la propia empresa, en su red interna, provocado o bien por empleados de la empresa, o porque la barrera del firewall ha sido insuficiente y el atacante ya está dentro. En este caso cobran importancia el uso de técnicas diferentes:

- **subdivisión** de la red mediante el uso de switches y hubs con características de seguridad
- sistemas de **monitoreo** de la red
- **seguridad en servidores.**

Seguridad en ambientes cliente/servidor

El uso de PCs como terminales inteligentes en un ambiente distribuido ha expuesto más los sistemas. El grado de esto depende del acceso físico y lógico al sistema, así como el valor de los datos y los programas accesibles.
La alta complejidad de los sistemas cliente/servidor se basan en:

- *contiene varios subsistemas diferentes que son todos de alta importancia para el*

funcionamiento del sistema total.
Por esta razón los requerimientos de protección se multiplican. Los subsistemas pueden ser de diferentes tipos, las instalaciones pueden estar en lugares diferentes, pero para proveer operación segura, los múltiples componentes centrales deben estar todos protegidos adecuadamente contra acceso físico no autorizado, uso ilegal, cambio o destrucción. Como los servidores de hoy en día son de dimensiones similares a un PC, se suele subestimar los requerimientos de protección; sin embargo estos deben ser acordes al tipo de aplicaciones y de datos que contenga.
Lo mismo sucede para los sistemas cliente, que se instalan con frecuencia como sistemas de usuario final. Estos puestos son de mayor importancia que las terminales ya que están equipados de inteligencia, y almacenamiento masivo

- *alta dependencia de los enlaces de red para la operación productiva*
  La flexibilidad y el desempeño de los sistemas cliente/servidor se basan en la interconexión de varias computadoras con diferentes tareas. Sin los enlaces de red, el sistema no puede funcionar, por lo que es de vital importancia la confiabilidad de la red, tanto para la operación del sistema como para su seguridad
- *las medidas de protección de los subsistemas deben coordinarse entre sí*
  Cada servidor u otra computadora con funciones claves en el sistema cliente/servidor debe ser protegido con un sistema de contraseñas. El acceso a programas y datos sólo debe ser posible con autorización explícita, y sólo se otorgará a los que lo necesiten para realizar su trabajo. Las medidas de seguridad deben ser consistentes en todos los subsistemas, como por ejemplo, un mismo usuario no puede tener diferentes tipos de privilegios, o cuando se va a borrar un usuario, los privilegios de éste deben ser eliminados de TODOS los subsistemas.
  El sistema entero es tan seguro como su parte más débil.
  Debe además haber un nivel parejo de seguridad física (protección del edificio, acceso físico, aire acondicionado) y operacional del sistema . Por ejemplo, es insuficiente que sólo algunos componentes estén conectados a UPS (sistemas de energía ininterrumpida)
- *operaciones de los componentes distribuidos deben coordinarse entre sí*
  En principio, los múltiples servidores, clientes, etc. permiten que un sistema cliente/servidor siga funcionando hasta cierto grado si falla uno de sus componentes. Sin embargo es de vital importancia para la integración de los resultados de proceso así como para la seguridad, que luego de una falla de alguna de las partes (hardware, software), se restablezca la concordancia entre los subsistemas.
  Debe haber procedimientos técnicos y organizacionales que aseguren que luego de una recuperación de una interrupción no planeada, los parámetros y definiciones para la protección de programas y datos estén en un estado correcto y sincronizado.
- *responsabilidad por las operaciones debe administrarse de forma centralizada*
  Debido a la necesidad de corrdinación entre los susbistemas conviene que ciertas tareas se manejen en forma centralizada: responsabilidad por las operaciones del sistema entero, por la administración de usuarios de todos los subsistemas, por la seguridad del sistema entero.
  Otro aspecto importante es la segregación de tareas aún en sistemas más pequeños. Las siguientes funciones deberían asignarse a diferentes personas:
  - desarrollo de sistemas
  - operación del sistema
  - autorización de usuarios
  - monitoreo de seguridad

Por otro lado, los privilegios de administración central y mantenimiento del sistema cliente/servidor deben otorgarse sólo si es requerido, al personal de TI, y su uso, dentro de lo posible, debe quedar automáticamente registrado (log)

Por años el standard mínimo de control de acceso ha sido el uso de contraseñas, pero hoy en día se han introducido nuevas técnicas de autenticación.
En un ambiente mainframe, las técnicas de procesamiento centralizado requieren que el usuario pase por una sola puerta para acceder al sistema.
Pero en un ambiente cliente/servidor existen varias puertas, puesto que los datos pueden existir en el servidor o en el cliente. Estos puntos de entrada pueden basarse en:

- *Cliente*: la estación de trabajo distribuida puede contener datos y/o la propia aplicación instalada en su/sus disco/s, de modo que para asegurar la estación de trabajo puede ser necesario usar paquetes de software de control basados en el acceso al PC. Una forma de asegurar el PC es deshabilitando la disquetera, para prevenir que alguien pueda saltearse el software de control. Otra posibilidad es asegurar los archivos batch de inicio de la PC, para que no puedan evitarse los scripts de acceso.
- *Red*: pueden usarse dispositivos de monitoreo de red para inspeccionar la actividad de fuentes conocidas o desconocidas. Para proteger datos sensibles se pueden usar técnicas de criptografía (clave pública y clave privada). Además, es recomendable el uso de fibra óptica en lugar de pares trenzados pues es más resistente. Sin embargo siguen habiendo amenazas derivadas por ejemplo del uso de analizadores de tráfico, que interceptan transmisiones.
- *Servidor*: algunas tarjetas usan dispositivos inteligentes “hand-held”, o criptografía para descifrar códigos aleatorios proporcionados por los sistemas operativos basados en cliente/servidor (por ejemplo UNIX). También existen programas de software que hacen lo mismo: se sincronizan inicialmente por usuario y luego se usan técnicas de criptografía para descifrar los códigos aleatorios.
- *Aplicación*: se limita el acceso de los usuarios tan sólo a las funciones que necesitan para desempeñar sus tareas. Se define el acceso en términos de los objetos a los cuales el usuario tiene autorización. En caso de intentos de violación, se puede bloquear la estación de trabajo, o desconectar la sesión, o emitir mensajes en algún log.

Autenticación

Es el proceso de verificar la identificación de un usuario. Puede depender de diferentes tipos de cosas, por ejemplo: una contraseña, una tarjeta, huellas digitales, o una combinación de ellas.

Contraseñas

Están expuestas a 2 tipos de riesgo:

- Exposición por descuido del usuario: por ejemplo, anotarla y dejarla a la vista, incluirla en un shortcut que invoque al programa, etc.

- Adquisición no autorizada: por ejemplo, ensayo y error hasta embocarle, métodos determinísticos o penetración en el sistema.

Fortaleza de una contraseña

Qué tan segura es en relación con los riesgos a los que está expuesta.
En la fortaleza de una contraseña influyen diferentes factores:

- Largo de la contraseña
- Número total de caracteres permitidos
- Si el proceso de adjudicación de contraseñas es lo suficientemente aleatorio.
- El grado de exposición a la vista: si está encriptada, o se despliega en pantalla cuando se entra.
- La disciplina impuesta a los usuarios

Dominio de las contraseñas

Es el conjunto de combinaciones posibles que pueden ser usadas para denegar el acceso a un sistema de información. Por ejemplo, si la contraseña sólo tiene hasta 4 caracteres, que deben ser letras mayúsculas, el espacio o dominio va a ser muy pequeño. Si en cambio, debe tener la misma cantidad de caracteres (4 caracteres), pero producidas aleatoriamente, se tiene un conjunto mucho mayor.

Desventajas de las contraseñas

- Los usuarios no siempre mantienen la confidencialidad
- Si un intruso logra pasar esta barrera, luego tiene el camino libre

Una forma efectiva de protección de contraseñas se obtiene mediante el uso de servidores de autenticación. Este almacena una clave única que corresponde a cada contraseña, y la contraseña es encriptada, es decir, convertida a texto cifrado, mediante un algoritmo. Este mismo algoritmo es usado para convertir el texto cifrado al texto normal. Necesita una clave para decirle a la ecuación matemática dónde comenzar a producir el texto cifrado.
El programa que descifra el texto necesita conocer esta clave. Las programas no deben ser codificadas con las claves.
El uso de claves encriptadas y algoritmos previene el acceso de usuarios casuales que quieran interceptar los mensajes.

Definición: Criptografía (Gallegos)

Es una técnica para crear información ininteligible a partir de información inteligible.
Se usa la misma técnica para descifrar el texto “encriptado”. El algoritmo utiliza una “clave” para crear la ecuación matemática para comenzar a producir el texto cifrado. Esta misma clave debe proveerse al programa que va a descifrar el texto.

Para que el método funcione, tanto el algoritmo como la clave deben mantenerse en secreto, y tampoco deben codificarse en el código fuente de los programas.

Definición: Autenticación

Autenticación significa establecer la prueba de identidad entre 2 o más entidades.

Tipos de autenticación

- Usuario a "host": proporciona acceso a usuarios a determinados servicios a los cuales tienen autorización, y les niega acceso a aquellos a los cuales no están autorizados.
  - *Contraseñas estáticas*
  - *Contraseñas por única vez*
  - *Terceros confiables*
- Host a host: tiene que ver con la identidad de computadoras en la red.
  - *No autenticación*: por ejemplo, autenticación basada en el nombre del host.
  - *uso de contraseñas*
  - *firmas digitales y criptografía*
- Usuario a usuario: establece la prueba de identidad de un usuario hacia otro.
  - *firmas digitales*
  - *Kerberos*

Areas de exposición

- Control del código fuente: hay 3 áreas de posibles debilidades:

1. si alguna porción de la seguridad se realiza en el cliente, estas medidas de seguridad podrían ser modificadas, por lo que es mejor poner esto en el servidor.
2. En segundo lugar, identificando el formato de invocaciones legítimas a la base de datos, se pueden escribir invocaciones no autorizadas, utilizando convenciones identificadas a partir del código fuente no-protegido, y enviarlas al servidor de base de datos, una vez conocida la dirección de red de la aplicación.
3. Pueden hacerse modificaciones no autorizadas al software de aplicación que se incluyen en el ambiente de producción la próxima vez que se recompilen y distribuyan los programas.

- Aspectos de autenticación: una vez que el usuario es autenticado, es importante asegurar que los requerimientos subsiguientes sean válidos. Esto puede realizarse capturando un paquete que envía un usuario identificado, modificando el requerimiento, reenviando el requerimiento, y luego interceptando la respuesta. Esto es bastante sofisticado pero posible. Para evitar problemas, lo mejor es reidentificarse periódicamente. Si se ha llegado al estándar DCE (Distributed Computing Environment) de la Open Software Foundation, esto no es necesario. Lo más destacable de esta norma es que el producto debe ofrecer un nivel suficiente de autenticación de usuario, como el que se obtiene con Kerberos.

- Conexión a la base de datos: es importante ver si el acceso a la base de datos es a través de un logon a la aplicación o un logon por cada individuo que usa la aplicación. Con la arquitectura three-tier, es muy probable que se haga un único logon de la aplicación, que provee acceso a todos los usuarios de la misma. Si este es el caso, la aplicación debe proveer seguridad interna para restringir el acceso a los individuos y funciones (agregar, borrar, sólo lectura). Individuos con acceso a la aplicación pueden tener sus propias identificaciones para conectarse tanto al servidor donde reside la base de datos, como a la base de datos. En este caso, la seguridad a nivel de aplicación puede no proporcionar el nivel deseado de control que originalmente se pensó. La lista de usuarios del servidor y la base de datos con privilegios de acceso debe ser revisada para detectar accesos conflictivos con la seguridad interna de la aplicación.

- Respaldo y restauración: En un ambiente cliente servidor, los datos pueden distribuirse para ubicarlos más cerca de quien los usa, reduciendo los tiempos de respuesta. Sin embargo, independientemente de dónde se guarden los datos, deben respaldarse. Si se almacenan localmente, hay 3 posibilidades:

    - Se respaldan localmente: hay que verificar que realmente se están respaldando, su frecuencia y dónde se guardan.
    - Se transmiten a través de la red para ser respaldados en un servidor centralizado de respaldos: hay un riesgo de tráfico excesivo en la red, que puede a veces evitarse haciendo los respaldos en horas no pico (por ejemplo de madrugada). Se resuelve el problema de que las cintas se guarden físicamente junto al servidor, siempre y cuando no se respalden además los servidores locales al centro de backup.
    - No se respaldan.

- Control de cambios de programas y migración: debe tenerse especial cuidado en la provisión de controles adecuados sobre la migración del ambiente de prueba a producción y subsiguiente distribución de nuevas versiones. Un punto significativo sobre la migración de versiones es que el software que ejecuta el cliente no necesariamente reside en el cliente cuando no se ejecuta. Puede ser bajado del servidor cuando se necesite. Esto aumenta el tráfico en la red pero facilita la distribución de un nuevo software. La mejor opción depende de cada caso.

- Consistencia del software del cliente: una aplicación que atienda múltiples departamentos o ubicaciones puede depender de la consistencia del sofware de base en cada puesto de trabajo. Si se libera una nueva versión que requiere un upgrade de este software, uno se puede encontrar con resistencia en las organizaciones por el gasto adicional, especialmente si no se ve ningún beneficio adicional para el departamento. En consecuencia los desarrolladores pueden verse forzados a mantener diferentes versiones, incrementando así los costos de mantenimiento.

- Aspectos de conectividad: esto es importante porque las aplicaciones cliente/servidor se

basan en las comunicaciones. Es posible que una estación de trabajo esté conectada a un servidor, que está en una red varios enrutadores más lejos (un "router" es un aparato que conecta segmentos de red entre sí). Este aparato consulta el tráfico para identificar la dirección de estaciones en la red. Estas ubicaciones las obtiene consultando las direcciones desde donde se originan los mensajes. No se mantiene una lista completa de direcciones puesto que ubicaciones poco usadas se eliminan de la tabla. Cuando llega una transacción cuya dirección no está en la tabla, se publica el requerimiento y luego cuando llega una respuesta, se actualiza la tabla. Si la aplicación no tiene un período de espera razonable, se le pasa un código de falla de comunicación y ésta debe retransmitir la transacción.

- Revisión del ambiente de desarrollo y prueba: un ambiente de prueba inseguro puede permitir modificaciones no autorizadas.

- Aspectos de sistema operativo: UNIX, Novel, NT.

- Problemas estándares:
  - Usuarios de instalación (como en el caso Oracle, el usuario SYS o SYSTEM), tienen contraseñas por defecto que deberían cambiarse.
  - Acceso de los programadores a los datos de producción, permitiendo cambios directamente sobre los datos
  - Usuarios con privilegios excesivos de lectura a datos sensibles de la empresa.
  - Ausencia de análisis de costo/beneficio de la empresa.
  - Fallas en la obtención de la aprobación del cliente al documento de especificación del sistema

Seguridad y Administración de una Intranet

Muchas organizaciones utilizan esta solución con el fin de agilitar la comunicación entre su personal, sobretodo cuando se trata de corporaciones multinacionales, con filiales muy distantes, y donde es necesario poner información del negocio a disposición del personal en el mínimo tiempo posible.

Definición

(Hinrichs, 1997)

Intranet es un sistema de información interno basado en tecnología Internet, servicios web, protocolos de comunicación TCP/IP y HTTP, y publicaciones en HTML.

Una Intranet es una red interna corporativa de una organización, usando las tecnologías que se desarrollan y aplican para Internet, con la intención de poner fácilmente disponible la información a una gran cantidad de usuarios. Típicamente se basan en TCP/IP, y se construyen sobre alguna de las siguientes tecnologías:

- World wide web

- Grupos
- Correo electrónico
- NetNews

El beneficio clave de usar esta tecnología proviene de que los usuarios de una organización pueden compartir información y colaborar electrónicamente sin importar la plataforma, ni ubicación ni fornteras.

Cliente/Servidor o Intranet

Comparemos las características de ambos ambientes:

	Cliente/Servidor	Intranet
Instalación	Instalación específica de un software cliente en cada estación de trabajo	Uso de un browser estándar para todas las aplicaciones de Internet [1]
Evolución de la aplicación	Actualización del cliente obligatoria	Sólo el servidor se actualiza
Modificación de estaciones de trabajo	Cuando se instalan nuevas aplicaciones, pueden haber incompatibilidades	Ningún impacto si el browser aún funciona
Evolución de la arquitectura de red	Parámetros en cada puesto deben ser actualizados (nombre del servidor, caminos de búsqueda)	Ningún impacto. Sólo los vínculos a la raíz de la aplicación deben ser actualizados en el servidor
Acceso desde oficinas remotas	Necesidad de gran ancho de banda a través de líneas rentadas	Posibilidad de usar Internet una vez resueltos los problemas de seguridad (firewall)
Tipos de estaciones de trabajo	Windows y PC	Cualquiera (PC, Mac, UNIX)

[1] Los web browsers tienen la ventaja adicional de ser una interface con la cual los usuarios cada vez se sienten más cómodos.

Características de las Intranet

1. Las Intranet permiten al usuario acceder a múltiples fuentes de información, proporcionando a la vez, una vista integrada de los datos, sin importar que residan en un mainframe, o servidor corporativo, un servidor departamental o un desktop de usuario. De modo que la información compartida puede originarse desde:

- Fuentes corporativas u organizacionales: tales como reportes anuales, políticas corporativas, procedimientos operativos, o descripciones de productos
- Individuos: tales como contribuciones a grupos de discusión, o requerimientos para un nuevo producto

- Sistemas operacionales: tales como órdenes de compra u órdenes de clientes

2. La información puede ser compartida e intercambiarse de muchas formas incluyendo texto, figuras, fotos y vídeo clips.

3. Las Intranet permiten que grupos de usuarios trabajen sin importar dónde están situados. De modo que, personas dispersas en todo el mundo pueden participar en discusiones, colaborar en proyectos, o simplemente interactuar sin importar su ubicación física.

Ejemplos de aplicación de Intranet

- ***Noticias organizacionales***: el control centralizado sobre el contenido hace que esta sea una primera aplicación relativamente segura y ayuda a la eliminación de costos de distribución e impresión.
  Análogamente, aplicaciones que "publican" pueden proporcionar facilidades tales como búsqueda en directorios corporativos, manuales de procedimientos para empleados e información de productos y precios para la fuerza de ventas.
- ***Flujo de trabajo mejorado***: todas las partes interesadas pueden colaborar y ver al instante el resultado.
- ***Herramientas de colaboración***: una base de datos de discusión organizacional puede proveer a los empleados de mecanismos para compartir sus ideas o hacer preguntas a otros empleados. Para una mejor utilización, la base de datos estará clasificada por asunto para poder enfocarse rápidamente en las áreas de interés.
- ***Acceso a aplicaciones ya existentes***: esto es útil para entregar información desde un sistema sin tener que proporcionarle a cada empleado una conexión a ese sistema.
- ***Aplicaciones híbridas***: combina varios de los anteriores. Por ejemplo, una aplicación de registro a un curso puede publicar un catálogo para que los potenciales estudiantes puedan fácilmente verlo o buscar un curso que satisfaga sus necesidades inmediatas. A partir de la página de información, puede haber un vínculo a un formulario de inscripción.

Desventaja de las Intranet

Hay un aspecto negativo en esta facilidad de compartir información y trabajar en forma interactiva, pues información corporativa tiene grados variables de confidencialidad. Por un lado hay información que puede publicarse en la página inicial de un periódico sin efectos adversos. En el otro extremo tenemos información que si se divulga fuera de un pequeño grupo, tendría un impacto en la reputación y/o rentabilidad de la organización. Sin los controles adecuados, la facilidad de acceso a la información proporcionada por la Intranet podría permitir que un usuario compilara y distribuyera cierta tal información – accidentalmente o deliberadamente – con mínimo esfuerzo.

Aspectos claves en la implementación de una Intranet

1. ***Estrategias en la elección de diseño de la aplicación***: qué herramientas de publicación, de colaboración, de correo electrónico y si se adoptan soluciones propietarias
2. ***Niveles de interacción***: cuánto trabajo se hace en el servidor (programas GCI) y cuánto en el cliente (Java, Active X)?

3. ***Características de seguridad embebidas***: el nivel de seguridad pre-construida dentro de los productos Intranet se relaciona con el aspecto propietario vs. Estándares abiertos. Mientras que los productos propietarios tienen una larga historia de fuerte seguridad pre-incluida (tales como control de acceso), los productos basados en estándares que usan protocolos abiertos, han surgido de un ambiente donde la seguridad, en el mejor de los casos era pensada después. Sin embargo, la convergencia de productos propietarios y basados en estándares está dirigiendo tanto a los proveedores como a los órganos que manejan los estándares hacia soluciones más seguras utilizando protocolos abiertos.

Desafíos de las aplicaciones de Intranet

La facilidad y disponibilidad de acceso a información de aplicaciones basadas en Intranet agrega algunas dimensiones nuevas a los aspectos a afrontar cuando usamos redes corporativas.

1. ***Permitir acceso externo a la Intranet para usuarios remotos***: aunque establecer una conexión con sitios remotos puede ser bastante sencillo, el fracaso en el manejo de la seguridad puede llevar a accesos no autorizados a información sensible, o que sea visible la información en tránsito, particularmente si las conexiones son hechas sobre Internet.
2. ***Acceso de terceros***: cuando se le quiere dar acceso a terceros (contratado, consultor, cliente o socio de negocio), el desafío es limitar el acceso de éstos a un subconjunto de la información de la organización que el usuario en particular necesita.
3. ***Control de acceso***: el acceso de Intranet a la información con frecuencia se implementa como un front-end de una aplicación antigua. Normalmente los niveles de seguridad de ambas partes no coinciden, por lo que la aplicación basada en web se trata como una aplicación confiable y se le otorga acceso relativamente ilimitado a la aplicación antigua. Esto puede ser un punto débil puesto que la aplicación web en general no fuerza el mismo nivel de seguridad.
4. ***Interface común a múltiples fuentes de información:*** la Intranet y el uso de un browser ofrecen la oportunidad de usar una interface común, consistente a múltiples fuentes de información. Sin embargo, desde el punto de vista del usuario, el aspecto de la información devuelta puede variar mucho.
5. ***La aplicación de soluciones de seguridad de Internet a Intranet***: con la seguridad de Internet, la estrategia con frecuencia es mantener una separación fuerte entre el "lado de afuera" y los sistemas que residen dentro de las fronteras de la organización. Sin embargo, como las Intranet con frecuencia cruzan las fronteras departamentales dentro de una organización, tal división puede ser contraproducente.

Planificación de una Intranet

Veremos una serie de aspectos a tener en cuenta cuando se prepara un caso de negocio y se planea introducir una intranet.

1. ***Definir alcance***: lo primero a tener en cuenta es el alcance y tamaño del proyecto:
   - *Aplicaciones a desarrollar*: cuáles aplicaciones se desarrollarán inicialmente, y qué criterios de selección se aplicarán en el futuro para las próximas aplicaciones.

- *Usuarios*: identificar los usuarios potenciales y la forma de autenticación y autorización
- *Conectividad*: deben definirse reglas firmes sobre cómo puede una intranet estar conectada a otras redes, particularmente a las externas como es el caso de Internet

2. ***Crear un caso de negocio***:
   - *Propósito de negocio*: debe reflejarse las necesidades de información del negocio en el diseño e implementación de una intranet. Es importante pensar cómo puede crecer una Intranet exitosa y evolucionar a medida que gana aceptación, potencialmente cambiando su propósito de negocio.
   - *Proceso de decisión*: debe existir una autoridad designada que preferentemente sea de la dirección para tomar decisiones en la planeación de la intranet, para que no se desvíe de los objetivos del negocio
   - *Cálculo del riesgo*: la falla en realizar un análisis de riesgo detallado puede llevar a la organización a pérdida o modificación no autorizada de información, acceso no autorizado y niveles inaceptables de disponibilidad del sistema.
   - *Integración de aspectos de seguridad al plan de negocios*
   - *Planeación de recursos*: se refiere no sólo a los equipos y componentes de software, sino también a los individuos necesarios para mantener la intranet.

Política de seguridad en Intranet

Como ya vimos, la seguridad es un medio de proteger la información, sin importar dónde resida, o si viaja en la Intranet.
De acuerdo a las estadísticas, de los fraudes relacionados con computadoras, 80% son cometidos por los usuarios internos. Además, es más fácil porque tienen el acceso, y conocen los controles de acceso a los recursos.

Elementos:

- Integridad: se reciben los datos exactamente como se enviaron
- Confiabilidad: se puede confiar en la integridad de los datos
- Disponibilidad: se puede acceder a los datos cuando lo necesita
- Seguridad: los datos están protegidos de accesos no autorizados

Definición de política de seguridad

Es un documento que describe los aspectos de seguridad de la red de una organización.

Aspectos en la definición de política de seguridad

- Planificación de seguridad de toda la red: vale la pena implementar la seguridad de la red si los recursos e información de la organización lo valen. Luego habrá que identificar los problemas de seguridad de la red y los tipos de servicios a los cuales se les permitirá acceder y a los que no, por razones de seguridad.
- Política de seguridad local de cada sitio: la política debe acompasarse a los objetivos

de cada sitio. Debe tener en cuenta la protección de los recursos:

- estaciones de trabajo
- computadoras centrales y servidores: routers, bridges, gateways
- dispositivos de interconexión
- software de red y de aplicación
- cables de red
- información en archivos y bases de datos

- Análisis de riesgos: debe ser considerado antes de moverse a una nueva plataforma, o extenderse. La gerencia necesita identificar los riesgos y emprender acciones para asegurar la privacidad de los datos de la organización.

Factores a tener en cuenta en la definición de la política de seguridad

- ***Identificar los recursos que trata de proteger la organización***: esto significa que se debe clasificar la información de acuerdo a su sensibilidad. Esto permite que los más interesados retengan la propiedad y el control sobre la divulgación y actualización de la información.
- ***Identificar de quiénes los quiere proteger.*** Esto implica:
  - establecer control de accesos, especialmente para usuarios remotos y los que no son empleados.
  - controlar quiénes pueden publicar información en la intranet.
  - Administrar los cambios de servicios y tecnologías.
- ***Determinar la probabilidad de las amenazas***
- ***Determinar las medidas:*** que puede implementar la organización para protegerse de una forma costo-efectiva. Significa que:
  - las medidas deben ser acordes a la importancia de los recursos y de la información.
  - la política debe incluir sanciones explícitas para los infractores.
  - Los estándares deben prepararse definiendo un nivel adecuado de entrenamiento en seguridad para todos los individuos que tengan acceso.
- ***Examen periódico***: de la política de seguridad de la red para detectar cambios en los objetivos de la organización y las circunstancias de la red
- ***Aspectos legales***: la amplia disponibilidad de información en una intranet, y la necesidad de protegela de accesos no autorizados pueden llevar a ciertos problemas legales difíciles de resolver, como por ejemplo:
  - Derechos de privacidad de los individuos
  - Derechos de autor
  - Uso internacional

Aspectos claves en la administración de una intranet

- ***Control de contenido:*** hay que restringir quiénes pueden publicar. Según la tecnología y plataforma utilizadas, cualquiera con conexión podría crear una página web personal y publicar información. Por lo tanto debe implementarse controles para impedir publicaciones

no autorizadas

- ***Control de acceso:*** debe proveerse una forma de auditar quiénes están accediendo y a qué.
- ***Protección contra virus:*** la facilidad de distribución de la intranet hace que este problema tenga una mayor incidencia, de modo que es muy importante implementar procedimientos estándares para la protección, detección y cura contra virus.
- ***Administración de la seguridad:*** debe contolarse el acceso y esto debe estar acompañado de configuración adecuada de estaciones de trabajo.
- ***Conectividad externa y control de acceso:*** una vez que las intranets de dos organizaciones están conectadas, la más fuerte puede heredar las debilidades de la otra. Si la más débil resulta comprometida, extraños no autorizados puede tener acceso a la más fuerte. También es posible que las comunicaciones de la red de una de las organizaciones sea monitoreada por individuos de la otra.
- ***Control de versiones de software de la intranet:*** continuamente salen al mercado nuevas versiones de los navegadores, pero la actualización apresurada puede dar problemas porque con frecuencia estas últimas versiones tienen errores y vulnerabilidades. Por otro lado, también hay que considerar la actualización masiva de muchos puestos de trabajo cuando es necesario aplicar un update que corrija estas debilidades.

Implementación de seguridad en Intranet

Aspectos

- Físico: por ejemplo, controles físicos y de procedimientos
- Red: aislamiento y particionamiento de red y encriptación de paquetes
- Plataforma: protección ante intrusos y herramientas de monitoreo.
- Seguridad de aplicación: autenticación fuerte, y comercio electrónico.

Etapas

1. Desarrollar una política de seguridad: lista de permitidos y prohibidos
2. Configurar los sistemas teniendo en cuenta la política de seguridad
3. Informar a los usuarios de los sistemas
4. Mantener los niveles de usuario y sistemas
5. Responder a las modificaciones que surjan

Post-Implementación de seguridad en Intranet

Es necesario hacer una revisión periódica de la política de seguridad. Además cambia la tecnología y la vulnerabilidad de las herramientas existentes.

Actividades de monitoreo

- Identificación de amenazas
- Chequeo de penetración
- Auditorías externas

Técnicas de seguridad en Intranet

1. Criptografía
2. Autenticación

Supervivencia: protección de los sistemas críticos

Redes ilimitadas como internet, no tienen una política de seguiridad única ni un control administrativo centralizado y unificado. Además, la cantidad y naturaleza de los nodos conectados a esa red no pueden ser completamente conocidos. A pesar de los grandes esfuerzos de quienes practican la seguridad, no se puede asegurar que un sistema conectado a esa red será totalmente invunerable a ataques. La disciplina de la Supervivencia puede ayudar a asegurar que estos sistemas puedan seguir proveyendo los servicios esenciales, y mantenet propiedades esenciales como la integridad, confidencialidad y desempeño a pesar de la presencia de intrusos. A diferencia de las medidas tradicionales de seguridad, que requieren control y administración central, la supervivencia está dirigida a los ambientes de redes ilimitadas.

Supervivencia en redes

Actualmente los sistemas de red de gran escala son altamente distribuidos y mejoran la eficiencia y efectividad de las organizaciones permitiendo nuevos niveles de integración en la organización. Sin embargo, tal integración está acompañada de riesgos elevados de aparición de intrusos y de que el sistema sea comprometido. Estos riesgos pueden ser mitigados incorporando habilidades de supervivencia en los sistemas de la organización. Como disciplina emergente, la supervivencia se basa en campso de estudio relacionados (ej:, seguridad, tolerancia a fallas, confiabilidad, reutilización, desempeño, verificación, y testeo) e introduce nuevos conceptos y principios.

El nuevo paradigma de red: Integración Organizacional

Desde sus modestos comienzos hace más de 20 años, las redes de computadoras se han vuelto un elemento crítico de la sociedad moderna. La mayoría de los sectores económicos, incluyendo las funciones gubernamentales, dependen de una gran cantidad de redes operando a escala local, nacional o global.
Las redes están siendo usadas para permitir mayores niveles de integración organizacional que eliminan las tradicionales barreras organizacionales e integra las operaciones locales con procesos del negocio basados en red. Por ejemplo,las organizaciones comerciales están integrando operaciones con unidades de negocio, proveedores, y clientes.

Definición de Supervivencia

Es la capacidad de un sistema de cumplir la misión de forma oportuna, en presencia de ataques, fallas, o accidentes. Usamos el término *sistema* en un sentido amplio, para incluir redes y sistemas de gran escala. En particular, el foco de la supervivencia está en los sistemas abiertos, sin límites donde las precauciones tradicionales de reguridad no son adecuadas.
El término *misión* se refiere a un conjunto de requerimientos u objetivos de muy alto nivel. Toda organización o projecto, para ser exitoso necesita definir una misión, es decir una visión de sus objetivos, ya sea expresados implícitamente o como una declaración formal. Juzgar si un sistema a cumplido o no su misión debe hacerse en elcontexto de factores típicamente hexógenos, que pueden afectar la normla

operativa. Por ejemplo, si un sistema financiero deja de funcionar por 12 horas durante un apagón muy extendido causado por un huracán, y ha preserrvado al integridad y confidencialidad de sus datos, y logra reanudar sus servicios más esenciales luego del incidente, se puede considferar que ha cumplido con su misión. Sin embargo, si el mismo sistema cae inesperadamente y está inoperante por 12 horas bajo condiciones normales o menores, y priva a sus usuarios de servicios financieros esenciales, el sistema, razonablemente puede considerarse como que falló en su misión, aún si se ha preservado la integridad y confidencialidad de los datos.
El tiempo es un factor crítico que normalement se incluye en los requerimientos de alto nivel para definir la misión. Sin embargo, el tiempo es un factor tan importante que se incluye explícitamente en la definición de supervivencia.

Es importante ver que lo que debe sobrevivir es el cumplimiento de la misión, no un subsistema en particular.

Características de los sistemas de Supervivencia

Propiedad	Descripción	Ejemplos
Resistencia a ataques	Estrategias para repeler ataques	Autenticación de usuario y del sistema, control de acceso, encriptación, firewalls, proxy servers, administración fuerte de configuración, dispersión de datos, diversificación de sistemas, aplicación de actualizaciones del sistema para vulnerabilidades conocidas
Reconocimiento de ataques y la extensión del daño	Estrategias para detectar ataques (incluyendo intrusión) y entender el estado actual del sistema, incluyendo evaluación de la magnitud del daño	Reconocimiento de patrones de uso de intrusión, exploración de virus, chequeo de integridad interna, auditoría, monitoreo de configuración del sistema, monitoreo de red
Recuperación de servicios esenciales y totales luego de un ataque	Estrategias para restaurar información o funcionalidad comprometida, limitando la magnitud del daño, manteniendo o restaurando servicios esenciales dentro de las restricciones de tiempo de la misión, restaurando completamente los servicios en la medida que las condiciones lo permitan	Restauración de datos y programas, uso de servicios alternativos, uso de modulos redundantes con la misma interface pero diferente implementación, procedimientos operacionales para restaurar configuraciones de sistemas, aislamiento del daño, habilidad de operar con servicios reducidos o comunidad de usuarios reducida
Adaptación y evolución para reducir efectividad de futuros ataques	Estrategias para mejorar la supervivencia de los sistemas basadas en el conocimiento ganado de ls intrusiones	Incorporación de nuevos patrones de reconocimiento de intrusos, registro y filtro adaptativo

Plan de recuperación de desastres o (contingencias)

Introducción

Importancia: fuerte dependencia de los Sistemas de Información

En los últimos años las empresas han incorporado cada vez más los avances tecnológicos, y sin duda el área de Tecnología Informática ha tenido una fuerte penetración en las organizaciones. Cada vez más dependen de los Sistemas de Información. Si bien esto trae muchos beneficios y posibilidades, también implica mayores riesgos de seguridad y control, y de aquí también la importancia de la "disponibilidad". Muchas empresas requieren hoy que sus sistemas trabajen en forma ininterrumpida. De aquí la importancia no solo del control de accesos de los usuarios o los posibles ataques externos, sino que también deben tomarse en cuenta los desastres naturales o no, pero que no son consecuencia directa del uso de los sistemas.
De acuerdo a un estudio hecho por la compañía Contingency Planning & Research en USA, entre 1992 y 1996 se reportaron 612 declaraciones de desastre, y las principales causas fueron:

101	Fallas de energía
87	Fallas de hardware
68	Fuego
60	Inundación
52	Huracán
44	Sofware
39	Bombas
38	Viento y nieve
23	Fallas en la red
44	Otros (huelgas, falta de equipo de apoyo, fugas en tuberías)

Si bien se puede argumentar que algunos de estos motivos son inaplicables en nuestro país, podemos ver que otras son universales (como es caso de fallas de hardware)

Además, no todos los desastres son naturales. El 75% de los desastres ocurren por factor humano:

- Empleados mal capacitados
- Mal diseño del sistema
- Empleados inconformes
- Fugas de información
- Mala administración del conocimiento
- Existencia de personal indispensable

Conclusiones

- Los negocios cada vez dependen más de sus Sistemas de información
- Importancia estratégica de los Sistemas de Información – ventaja competitiva. No son solo económicos los daños que una empresa sufre ante una situación de desastre, sino que también se daña su imagen. Perder la oportunidad de atender a un cliente significa darle ventaja a la competencia.
- Importancia de la "disponibilidad" en sectores competitivos: por ejemplo, en México existen Bancos que llegan a tener promedios de hasta medio millón de transacciones por día, que en caso de no realizarse podrían representarles hasta 50 millones de dólares en pérdidas.
- Necesidad de garantizar la continuidad del servicio
- Complejidad creciente de los Sistemas de Información
- Aumento de las amenazas (riesgos)
- Necesidad de pensar más allá de la prevención: ¿qué hacer, si pese a la prevención, la contingencia sucede? Crear un plan de recuperación de desastres implica contemplar todas las posibles fallas y situaciones de emergencia en un centro de cómputos, y establecer medidas para que en caso de que algo suceda, éste sea reactivado en el menor tiempo posible.

Implementación de un plan de contingencia

Preguntas a hacerse

- *¿Tiene disponible un plan de Recuperación de desastres ?*
- *¿Hay una persona encargada como responsable de la recuperación?*
- *¿Se han identificado los requerimientos mínimos de hardware, software, comunicaciones, y recursos humanos para la recuperación?*
- *¿Se ha definido el equipo de recuperación y han recibido entrenamiento?*
- *¿Tiene almacenamiento externo de sus datos vitales?*
- *¿Realiza inspecciones periódicas en relación de la capacidad y seguridad de su área?*
- *¿Existe una política de backup para usuario final?*
- *¿Restringe el acceso físico a sus instalaciones?*
- *¿Tiene prevista una instalación alternativa de procesamiento de datos?*
- *¿Ha sido probada?*

Objetivo

- Permanecer activo aún después de un desastre
- Prevención
- Asegurar la disponibilidad y confiabilidad de los Sistemas de Información
- Controlar la confusión, minimizando la posibilidad de cometer errores y reduciendo las pérdidas debidas al tiempo de interrupción.

Metodología

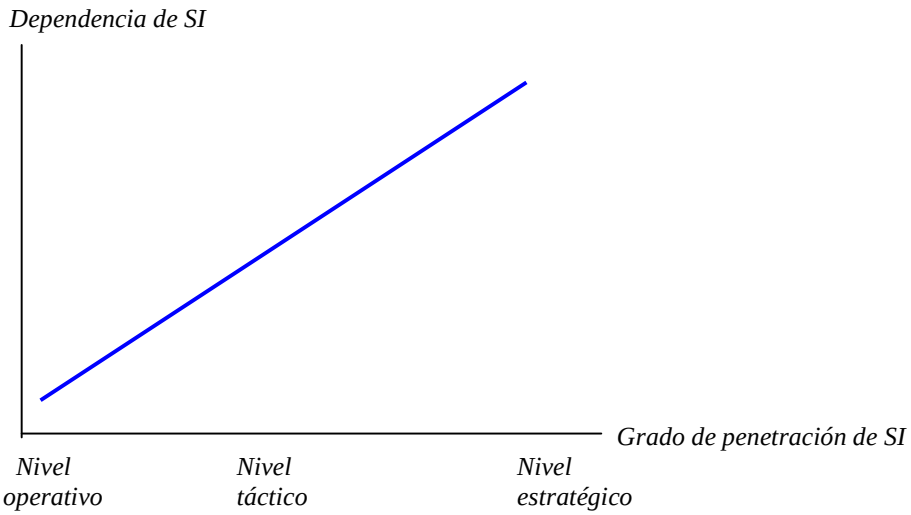
- Análisis de Riesgos: pérdida de capacidad operacional, deterioro de la organización

  - *Medir*

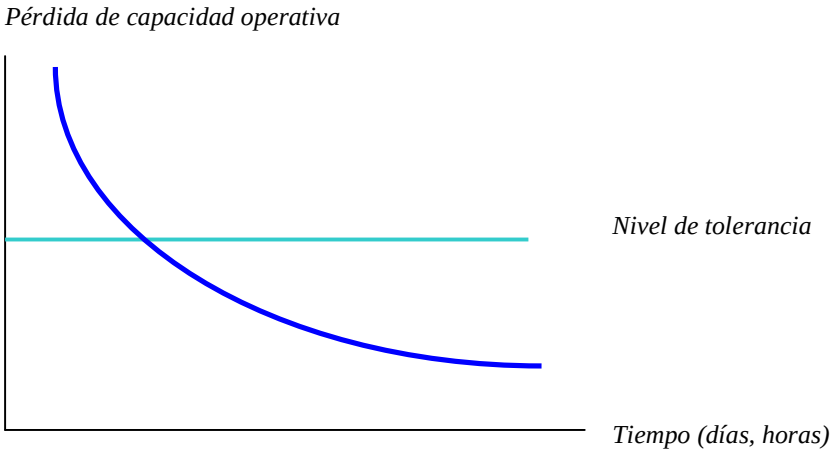
  Exposición = costo estimado de la pérdida producida * frecuencia de que suceda

  Estos valores pueden ayudar a la toma de decisiones sobre qué acciones tomar: asumir el riesgo, contratar pólizas de seguro, o implementar medidas adecuadas a las situaciones.

  - *Evaluar*



1. Análisis de la dependencia de las organizaciones de sus SI – comparar con grado de penetración de los SI (en los distintos niveles de toma de decisión)
2. Requerimientos legales
3. Requerimientos operativos del sector donde opera la empresa
4. Requerimientos corporativos
5. Deterioro de la organización luego de la ocurrencia de un desastre – comparar la pérdida de capacidad operacional con la dependencia de los SI: concepto de “nivel de tolerancia” ante la interrupción del servicio



DESASTRE: cualquier evento interno o externo que interrumpa el funcionamiento del área deTI por un período mayor a su nivel de tolerancia, comprometiendo así la continuidad del negocio.

- *Determinar posibles contingencias: seleccionar las amenazas más relevantes*
  Fallas en los equipos
  Interrupción/fallas en telecomunicaciones
  Interrupción de suministro de energía eléctrica
  Incendios
  Otros

- Educación de los usuarios

Etapas

1. *Inicio del proyecto*
   - Conseguir el apoyo real de la alta gerencia, haciendo que tome conciencia del problema y sus implicancias para el negocio, comprometiéndola para que el proyecto sea viable.
   - Designación de responsables: equipo de trabajo
   - Identificación de aplicaciones críticas
   - Identificación de tiempos críticos (horarios, días)
   - Identificación de amenazas (posibles contingencias)
   - Identificación de áreas de exposición (riesgo):
     - Fallas de hard/software (redundancia, respaldos/recuperación)
     - Protección de redes: Internet y Web, Virus, E-mail, telecomunicaciones (Firewalls, Antivirus y actualizaciones, criptografía)
     - Protección de mainframes
     - Protección del lugar físico
   - Análisis de riesgos
   - Desarrollo de una política de continuidad del negocio que abarque todas las áreas, pero que haga hincapié en las funciones críticas.
   - Acuerdos recíprocos

2. *Desarrollo del plan*

   Instrumentar acciones que permitan garantizar la seguridad física de los empleados y los bienes de la empresa, así como el restablecimiento de los servicios de TI dentro del plazo determinado por el nivel de tolerancia.

   - Análisis de riesgos
   - Identificación de funciones críticas y aplicaciones críticas
   - Identificación de recursos críticos y procedimientos alternativos para superar la contingencia.
   - Factores críticos:
     - sitio de procesamiento alternativo
     - sitio externo para almacenamiento de respaldos
   - Definición de procedimientos de Emergencia:
     - Evacuación
     - Prácticas de primeros auxilios
     - Restauración de datos
     - Conexión de líneas de comunicaciones alternativas
     - Instalación de "routers", etc.

     Involucra personas de distintas áreas, por lo que es conveniente definir diferentes grupos de trabajo con distintas responsabilidades y objetivos concretos
   - Proceso para declarar una contingencia: ¿en qué circunstancias?
   - Tiempos para declarar una contingencia: ¿cuándo hacerlo?
   - ¿Quién puede declarar una contingencia?
   - Evaluación de distintas alternativas

3. *Documentación del plan*
   - Por escrito
   - Distribución de copias a las personas responsables
   - Claro y fácil de entender

4. *Prueba y mantenimiento de las medidas de seguridad*

   Ciclo de prueba:
   - Definición de resultados esperados
   - Prueba: de adaptación y de cumplimiento.
   - Medición de desvíos
   - Evaluación de los resultados y posibles mejoras
   - Modificación del Plan

   Mantenimiento:
   - Programado: para comprobar la validez del Plan, por ejemplo, cambio del teléfono particular de una persona importante a la hora de la contingencia, cambio de lugar de trabajo de alguien, cambio en las condiciones contractuales de un proveedor, o cambio de proveedor.
   - Eventual: ante cambios de plataforma, de sistema operativo, puesta en producción de nuevas aplicaciones, o reemplazo de aplicaciones por nuevas versiones,

apertura de nuevos locales de la empresa, o mudanza, etc.

APÉNDICE

Conceptos de ambientes cliente/servidor

Las diferentes plataformas que una aplicación puede involucrar van desde las estaciones de trabajo tipo PC, los servidores de red (LAN), equipos de mediano porte tipo IBM AS/400, hasta los mainframes.

Generalidades

Una implementación cliente/servidor emplea múltiples procesadores para realizar su tarea. Los distintos componentes de la tarea se dividen entre los procesadores disponibles de modo de optimizar la capacidad de cada uno, y la disponibilidad de la red.
Veamos 2 casos típicos:

- Two-tier: el software se ubica en la estación de trabajo, que maneja toda la funcionalidad de la aplicación, incluyendo la seguridad. Esta aplicación accede a la segunda plataforma, que usualmente es una base de datos ubicada en un servidor de red. En esta instancia, la actividad es dirigida por la estación de trabajo.
- Three-tier: es más limitado en su alcance. Proporciona interface gráfica de usuarios, y puede realizar algunos procesamientos de datos simples como edición preliminar de campos. La funcionalidad primaria reside en el servidor (2a. "pata"), y los datos residen en otro/otros servidor/es.

Componentes de una aplicación cliente/servidor

- Software de desarrollo: lenguaje o ambiente usado para construir la aplicación.
- Software aplicativo: es el código de la aplicación misma. Puede residir en el servidor o en la estación de trabajo.
- Invocación a procedimientos remotos: es un proceso o transacción formateado en una plataforma, y enviado para su ejecución en una segunda plataforma.
- Base de datos: donde residen los datos de la aplicación, que puede ser un servidor, o puede estar distribuida entre varios. Se accede mediante invocación a procedimientos remotos.
- Protocolo de red: por ejemplo tcp/ip (Transmission Control Protocol/Internet Protocol), que ha sido diseñado abierto e independiente de las plataformas, o IPX de Novell (Internetwork Packet Exchange)
- Middleware: es un software que interactúa entre los módulos ejecutables y el protocolo de red, de modo que la aplicación y el software de desarrollo puedan ver la red en forma transparente.
- Sistemas operativos: DOS, Windows, OS/2, Netware, Unix, MVS, VM, etc.
- Servidores: entre sus funciones podemos destacar servidores de archivo, de impresiones, de acceso a bases de datos, de comunicaciones, etc.
- Estaciones de trabajo: es la máquina cliente que proporciona la interface gráfica.
- Rutina enrutadora: los requerimientos hechos por las rutinas cliente/servidor pueden ser a diferentes servidores, de modo que se necesita una rutina que conozca cuáles son y cómo dirigirse a ellos.

Uso de la tecnología cliente/servidor

Ventajas

1. Descargar procesamiento a máquinas más baratas. El costo por Millones de Instrucciones Por Segundo (MIPS) es menor a medida que se pasa de mainframes a plataformas más chicas.
2. Colocar datos cerca del usuario, y bajo el control de éste, descentralizando la función de IT.
3. Facilidad para obtener Sistemas Abiertos, que permite que productos de distintos vendedores puedan interactuar con una interface standard.
4. Habilidad para crecimiento progresivo de aplicaciones: por ejemplo, agregar un nuevo servidor.
5. Reducir el tráfico de red: existe la oportunidad de enviar transacciones y respuestas en vez de grandes bloques

de datos, además de la presentación en pantalla se puede encargar el cliente.

Desventajas

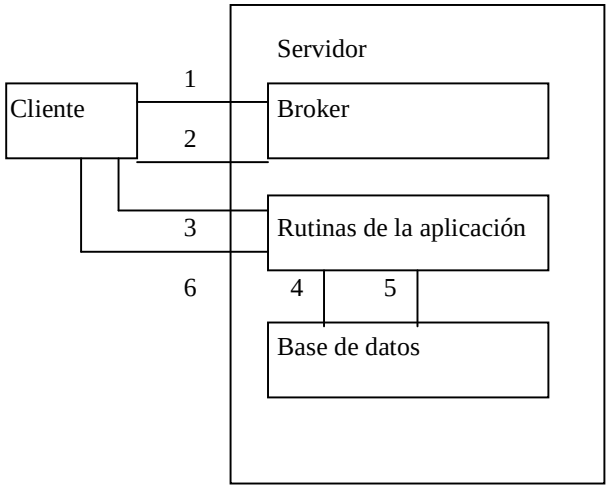
1. EL procesamiento puede no ser más barato (por ejemplo, al sustituir terminales tontas por workstations poderosas, el costo por puesto de trabajo puede aumentar considerablemente).
2. Control de los datos por parte del cliente: las técnicas de respaldo y restauración utilizadas pueden no cubrir los puestos de trabajo.
3. Una aplicación cliente/servidor mal diseñada, en vez de ahorrar tráfico en la red, puede paralizarla.

Arquitectura three-tier

Pasos en el proceso de conexión:

1. El cliente inicia la aplicación en la estación de trabajo. La aplicación le pide el usuario y contraseña, que se almacenan hasta que se necesiten. Se emite un RPC (logon request call) al "application-broker".
2. Se le devuelve al cliente la dirección de red utilizada para el chequeo de seguridad. El cliente formatea el requerimiento del servidor, e incluye el usuario y contraseña y la dirección de red recibida.
3. Se envía la transacción a la porción de la aplicación del servidor para ser procesada.
4. El servidor consulta la base de datos de seguridad para ver si el usuario y contraseña son válidos.
5. Cuando se completa la autenticación, se consigue información adicional como el código de organización o las limitaciones en el acceso.
6. El servidor envía un mensaje de aceptación o rechazo al cliente, con alguna información adicional obtenida de la base de datos.

A continuación vemos gráficamente cómo interactúan los distintos componentes:



Una vez que el usuario es autenticado, se siguen los siguientes pasos para manejar las transacciones subsiguientes:

1. Se saltea este paso, puesto que el cliente ya tiene la dirección de red necesaria.
2. Idem (1)
3. Los requerimientos, como por ejemplo agregar, borrar o modificar, se pasan al servidor. No se realizan chequeos de autenticidad, puesto que el usuario ya ha sido identificado.
4. Se accede a la base de datos para satisfacer la porción de datos del requerimiento.
5. Una vez completada la consulta, se formatea la respuesta

õ Se notifica a la estación de trabajo sobre la finalización de la tarea y se le envía al cliente los datos que éste haya requerido.

Técnicas de autenticación

- Encriptación de claves públicas: una entidad de red dispone de su clave privada (usada para encriptar y descifrar información y mensajes antes de enviarlos). Cada clave privada tiene asociada una clave pública que cualquiera puede usar para encriptar mensajes. El que envía arma el mensaje con la clave pública del destinatario. Y el destinatario lo descifra con su clave privada. Este método sirve también para asegurarse de que el mensaje llegue completo, y se usa mucho debido al gran crecimiento del manejo electrónico de las transacciones.

- Autenticación única (single sign-on): es mejor tener una sola contraseña para acceder a múltiples plataformas, porque de lo contrario, es difícil acordarse, y uno tiende a escribir las contraseñas. Hay diferentes productos en el mercado que manejan esto, por ejemplo, encriptando todas las contraseñas de cada usuario para cada plataforma. La desventaja es que crea un punto potencial de falla único, además de cuellos de botella en la red.

- Kerberos: se basa en la idea de que tanto el que envía como el destinatario, deben ser conocidos por un tercero (Kerberos). Usa un servidor de autenticación que valida la contraseña del usuario y emite "tickets" de acceso para ingresar a otras máquinas en la red. Al igual que en la encriptación de claves públicas y privadas, usa claves para transmitir paquetes de datos utilizando el algoritmo DES (Data Encryption Standard). Tiene 3 componentes básicos:

    - Base de datos: usuarios habilitados
    - Servidor de autenticación: determina si el user ID existe en la base de datos
    - Servidor que emite tickets: para acceder sólo al servidor solicitado

  Como Kerberos no transmite las contraseñas a través de la red, el usuario no puede cambiarlo por sí solo, y en consecuencia, no se pueden aplicar muchos de los procedimientos de seguridad de contraseñas. Además, el DES tiene debilidades. Como para asegurar una red grande, el número de claves requeridas es poco práctico, se utiliza encriptación de claves privadas compartida en ambientes cliente/servidor. En este caso, cada cliente y servidor, comparten el mismo método de encriptación y clave.

Tipos de "Firewalls"

1. Filtrado de paquetes

Utiliza routers con reglas de filtrado de paquetes que otorga o niega acceso, basado en la dirección origen, y la dirección y puerto destino.

Ventajas

- barato
- apropiado para ambientes con bajo nivel de riesgo
- rápido
- flexible
- transparente

Desventajas

- la dirección y puerto contenido en el paquete IP es la única información que dispone el router
- no protege contra modificaciones de IP o DNS
- un intruso tiene acceso directo a cualquier host o servidor luego de pasar esta barrera.

2. Nivel de circuito

Valida TCP, y en algunos productos UDP (User Datagram Protocol), antes de establecer una conexión o circuito a través del firewall.

Se monitorea el estado de la sesión y se permite el tráfico sólo mientras la sesión esté abierta.

Desventajas
Si no soporta UDP, no puede soportar tráfico UDP nativo o DNS (Domain Name Service) y SNMP.

3. Aplicación

Utiliza programas de servidor (proxies), que toman requerimientos externos, los examinan y en caso de que sean legítimos, los envían al host interno que proporciona el servicio apropiado.

Ventajas
- Puede configurarse como la única dirección de host visible para la red exterior, requiriendo que todas las conexiones hacia/desde el exterior pasen por el firewall
- Previene el acceso directo a servicios de la red interna, utilizando proxies para diferentes servicios (como FTP, HTTP, etc.)
- Proporcionan una historia de eventos al nivel de usuario

4. Híbridos o complejos

Combina 2 o más de los métodos anteriores, utilizándolos en serie, de modo que se puede mejorar la seguridad de la red. Es apropiado para ambientes de mediano a alto riesgo.

Tipos de "Firewalls" (otra clasificación)

1. Multi-homed host

Es un firewall que contiene más de una interface de red, conectando cada una de ellas a segmentos de red lógicamente o físicamente separados.
Cuando hay dos interfaces, se dice que es "dual": tiene dos tarjetas de internase de red, cada una de las cuales va conectada a dos redes, por ejemplo, una a la red exterior, y otra a la interna.

2. Screened host

Utiliza un host al que se conectan todos los host externos.

3. Screened subnet

Utiliza un host al que se conectan todos los host externos, y además crea una red separada de la red interna, donde reside el firewall. De esta manera, si un intruso logra entrar, queda supeditado al "perímetro" de esta sub-red.

Bibliografía

- *Administración* – James A.F.Stoner, R.Edward Freeman
- *Empresas/400* – N°7 de Editores Asociados de América S.A. de C.V. (junio/julio 1998)
- *Empresas/400* – N°9 de Editores Asociados de América S.A. de C.V. (octubre/noviembre 1998)
- *Servucción , El marketing de servicios* – Pierre Eiglier, Eric Langeard
- *Percepciones* – N°1 de Information Systems Audit and Control Association (ISACA, 1998)
- *IS Audit & Control Journal* – Volume III(ISACA, 1994)
- *IS Audit & Control Journal* – Volume IV (ISACA, 1995)

Sitios web de referencia

- *Handbook of Information Security Management: Policies, Standards, and Organization* – http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf http://www.windowsecurity.com/whitepapers/policy_and_standards/
- Quality Control in Service Industries - http://www.juran.com/elifeline/elifefiles/2009/11/Quality-Control-in-Service-Industries_JMJuran-94.pdf
- DOD Guidelines in Data Quality Management – http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%201996/Papers/DODGuidelinesonDataQualityManagement.pdf
- http://www.cert.org
- www.isaca.org
- https://www.enisa.europa.eu/