I : INTRODUCCIÓN

La Seguridad Informática nace como la necesidad de protección de los activos, tangibles e intangibles, que las organizaciones ponen en manos de una herramienta de gran poder y extrema debilidad.

Sin duda el crecimiento explosivo del Hardware y en menor medida del Software, ha sometido a las organizaciones a la dictadura de la Informática, sin cuya eficiencia ya no se concibe su actuación en un mercado moderno y competitivo; pero al mismo tiempo la falta de conceptos de Seguridad respecto a las ventajas comerciales que la provisión indiscriminada de elementos informáticos aporta a sus fabricantes, ha dejado a las organizaciones en un estado de indefensión ante ataques a la confidencialidad, la integridad y hasta la confiabilidad de las informaciones que manejan.

Al comenzar a reconocerse estos fenómenos, la especialidad tiene un gran crecimiento en los últimos años y se puede pronosticar que lo tendrá aún mayor cuando se generalice en la conciencia de los usuarios la importancia de tener niveles de seguridad adecuados no sólo en el procesamiento de sus datos, sino también en todos los aspectos asociados, desde el Gerenciamiento del área hasta el diseño de las instalaciones secundarias, dado que es en el conjunto de actividades informáticas donde reside la mayor probabilidad de daño por funcionalidad inadecuada o permeabilidad a los ataques externos que deba soportar cualquier organización.

En el estudio de esta especialidad también se han cometido errores, propios del inicio de una técnica aún difusa en muchos de sus aspectos. Por ejemplo, la mayor parte de la bibliografía pretende asociar la Seguridad Informática casi exclusivamente a la Criptografía y a sus algoritmos funcionales, dejando de lado otros aspectos de tanta o mayor importancia. El presente trabajo trata de aunar todos los conceptos interdisciplinarios que comprende la especialidad, asociando la experiencia, la teoría y las novedades que surgen permanentemente, dejando aclarado que cada nuevo producto que aparece en el campo informático deberá tener su nuevo y propio estudio de Seguridad, que adapte las actuales técnicas activas y pasivas a las características de sus innovaciones.

Finalmente, debe recordarse que la Seguridad Informática es básicamente un concepto y como tal depende de quien la aplique; sin duda el punto mas importante es la inclusión de sus pautas en el Diseño de los Sistemas, el cual, además de lograr eficiencia utilizando al máximo las herramientas que las configuraciones disponibles le ofrezcan, debe

contemplar las aplicaciones de Seguridad que esas configuraciones ofrecen y completarlas con las propias características operativas del Sistema en caso de ser necesario.

I.1 IMPORTANCIA DE LAS FALLAS EN INFORMÁTICA:

porqué es tan importante contemplar estas fallas:

- ✓ por la multiplicidad de uso de los sistemas informáticos, que abarcan prácticamente todo el espectro administrativo técnico de una empresa
- ✓ por la falta de los procedimientos alternativos, que normalmente se desechan al implementar Sistemas informatizados
- ✓ por el software amigable, que da acceso a informaciones y procesos importantes a quienes no siempre están capacitados para usarlos
- ✓ por la expansión del propio trabajo, lo cual implica una mayor dificultad en el control al disponerse de herramientas que no se dominan totalmente
- ✓ por el fácil acceso a grandes volúmenes de información, lo que produce la dicotomía de limitarlo y perder eficiencia o liberarlo y dejar la Seguridad al albedrío del usuario

Ejemplo: Calificación del BCRA para entidades financieras:

En el sistema existen distintos requisitos:

- requisitos de capital
- requisitos operativos
- requisitos de efectivo mínimo
- requisitos para las relaciones comerciales
- requisitos de sistemas (seguridad informáticas) → *representa un elevado porcentaje debido a la importancia fundamental de la información en la actividad financiera*

I.2 SEGURIDAD vs. COSTOS:

La Seguridad siempre implica gastos adicionales a la operación de la empresa, lo que dificulta su aceptación en principio, ya que para lograr competitividad muchas empresas prefieren mantener sus costos bajos a expensas de su seguridad interna; al no gastar en controles aumentan los riesgos principalmente por:

- facilidad de ataques
- falta del dominio de la tecnología (cambios frecuentes)
- alta dependencia de terceros (software y hardware)
- intervención de entes externos (ATM, Internet, TJ crédito y débito)
- dificultad para mantener la confidencialidad de la información

I.3 DEFINICIÓN GENERAL DE SEGURIDAD:

"Seguridad es todo aquello que permite defenderse de una amenaza".

Se considera que algo está seguro si ninguna amenaza se cierne sobre ello o el riesgo que las existentes lleguen a materializarse es despreciable.

I.4 DEFINICIÓN DE SEGURIDAD INFORMÁTICA:

"***Es la rama de la Seguridad que se ocupa de los procesos informáticos, su operación, diseño y correlación con los Sistemas Administrativos en los que actúan".***

En la Seguridad Informática son evaluados fundamentalmente los riesgos en el Diseño y la Operación de los Sistemas Informáticos, tratando de lograr un equilibrio entre el costo de los controles necesarios para evitar que los procesos se conviertan en amenazas y el costo de la concreción de las mismas. La importancia de los daños que se pueden causar esta dado no sólo por la importancia de los Sistemas Informáticos ya descripta sino también por la variedad de sus causas, yendo desde errores humanos hasta sabotajes, robos de información, cataclismos, fraudes, fallos en equipos y virus.

I.5 EVOLUCIÓN DEL RIESGO INFORMÁTICO:

- '70: seguridad en manos del System Programmer (una persona especilizada en Sistemas Operativos de grandes equipos que se encarga de administrar la seguridad)

- '80: se difunde la PC. Se distribuye el procesamiento (Redes - Multitarea), la seguridad baja al diluirse la responsabilidad entre muchos poseedores de la información y la facilidad con que pueden procesarla sin conocimientos profundos. La relación autoridad – responsabilidad, que es básica en una buena administración de cualquier organización, debe tomar formas distintas a riesgo de perder su equilibrio

- '90: proliferan las redes LAN, los virus y aparece Internet; todo tiene un gran criterio comercial, pero sin seguridad. Sólo a fines de los '90 se le da real importancia a este tema, partiendo de la Auditoría Informática en las entidades financieras

- '00: principalmente por los problemas con Internet se transforma la Seguridad Informática en una necesidad. Se popularizan las medidas de prevención, cifrado, criptoanálisis, firma digital y las autoridades de certificación aplicadas a las redes de ATM y el e-comerce

I.6 SEGURIDAD FÍSICA Y LÓGICA:

- Seguridad Física:

Es la protección ante las amenazas físicas de instalaciones, equipo, datos, software de base y aplicativo, personal y documentación.

- Técnicas de Seguridad Física:
  - diseño de instalaciones
  - restricciones al acceso de personal
  - protección contra incendios
  - resguardos contra agresiones físicas
  - catástrofes

- servicios auxiliares
- tolerancia a fallos
- resguardos (back up) y recuperación
- especificaciones de contratos
- seguros

- Seguridad Lógica:

Es la protección de la información, en su propio medio, contra robo o destrucción, copia o difusión. Se usa la criptografía, firma digital, administración de seguridad y limitación de accesibilidad del usuario.

I.7 OBJETIVOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA:

a) Confidencialidad: Que la información llegue en cantidad, calidad y oportunidad sólo y a todos los que está previsto.

   El quiebre de la confidencialidad puede traer consecuencias en:

   - pérdida de tecnología (espionaje industrial)
   - trabas en el funcionamiento de la organización que puede llevar al caos
   - pérdida de clientes
   - pérdida de oportunidades
   - pérdidas por acciones legales por no preservar secretos (bancos)
   - descontento interno al conocerse parcialmente o deformadas las políticas (racionalización)
   - pérdida de inversiones, por desconfianza en la seriedad de la empresa

b) Integralidad: Se refiere a que la información producida tiene los contenidos en calidad y cantidad con que fue diseñada (contrario a fraude).

Los efectos perjudiciales pueden ser mucho mayores que sobre la confidencialidad dado que puede tardarse mucho tiempo en detectar el ataque (ejemplo: redondeos, descuentos a clientes).

c) Disponibilidad: Es la oportunidad en la cual se dispone de la información. Completa el concepto de Integralidad.

I.8 SEGURIDAD ACTIVA Y PASIVA:

- Seguridad Activa: es aquella cuyas medidas tienen como objetivo anular o reducir los riesgos existentes o sus consecuencias para el sistema.

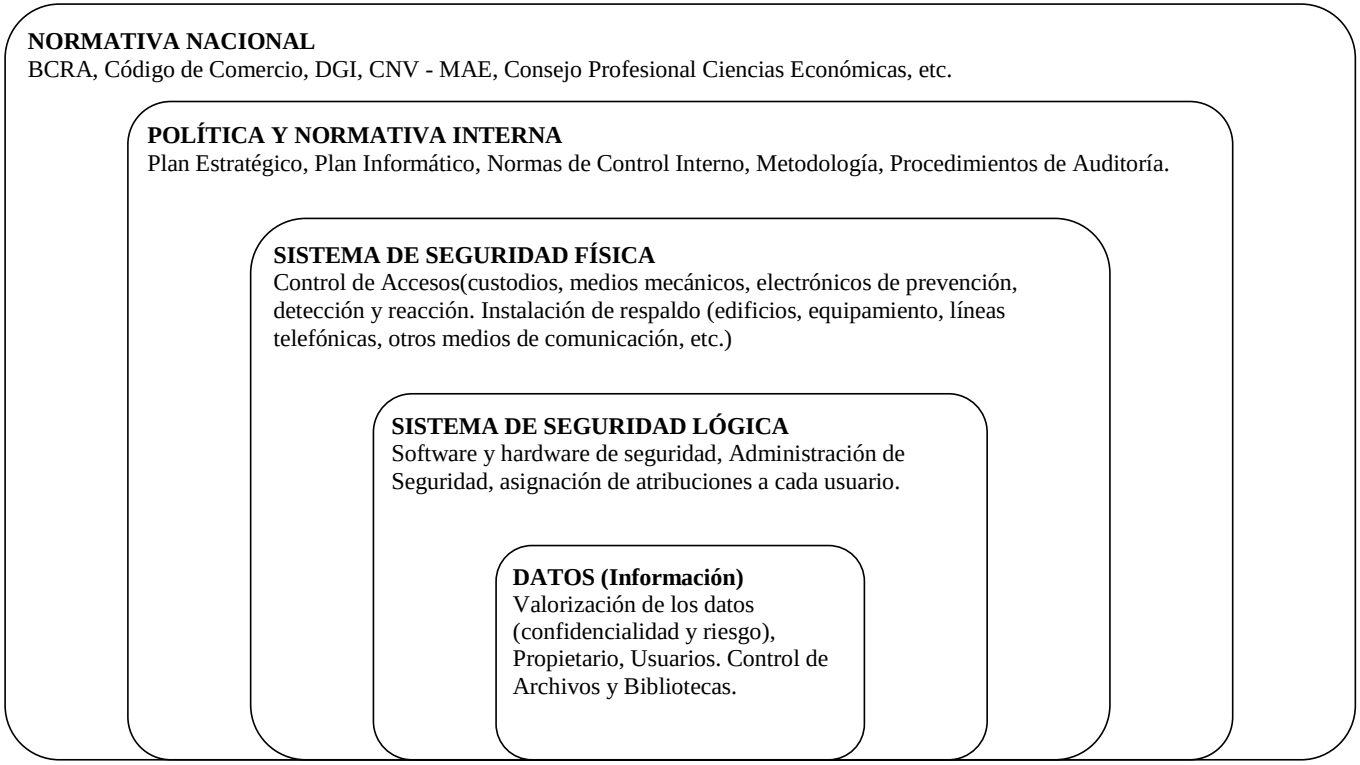
- Seguridad Pasiva: es aquella que prepara al sistema para el caso en que el desastre que amenazaba el riesgo se haya producido; ejemplo, sistemas de back-up.

I.9 CUADRO GENERAL DE AMENAZAS Y MEDIDAS A TOMAR EN SEGURIDAD ACTIVA Y PASIVA:

A M E N A Z A S	**S E G U R I D A D A C T I V A**	**S E G U R I D A D P A S I V A**
Errores humanos	• formación o capacitación • asignación adecuada de los permisos de acceso a los datos.	• controles de asiduidad de errores para producir el reemplazo de personal
Robo o alteración de la información del sistema	• autenticación de los usuarios • elección de claves seguras y mantenimiento en secreto • asignación adecuada de los permisos de acceso a los objetos • establecer alarmas sobre eventos • utilizar programas de bloqueo cuando haya que dejar el sistema desatendido	• cambios en el cifrado • estudio de los registros de auditoría
Robo o alternación de la información en la transmisión	• utilización de canales seguros • disponibilidad de canales alternativos • cifrados confiables	• cambios en el cifrado y en los canales en uso
Robo de los equipos	• acceso restringido a los equipos • fijación de equipos a soportes •	• copias de seguridad • equipos de reserva • anotar modelos y números de serie • revisión de las presencias en la sala • marcación de los equipos

AMENAZAS(cont.)	**SEGURIDAD ACTIVA**	**SEGURIDAD PASIVA**
Fallo en el suministro eléctrico	• revisión y control de redes • líneas de suministro alternativo	• UPS • supresores de picos de tensión • generación propia de energía eléctrica
Desastre natural	• estudios geo – meteorológicos de la zona • estudio del lay-out de los centros de cómputos	• copias de seguridad • almacenamiento los BU en ignífugos • tener equipos de reserva • asegurar los equipos
Recepción de información falsa	• autenticación de la información mediante firmas digitales	• cambios en el cifrado
Sabotaje de los equipos	• acceso restringido a los equipos	• equipos de reserva • copias de seguridad • equipos de reserva • revisión de las presencias en la sala
Sabotaje de la información	• acceso restringido al sistema • asignación adecuada de los permisos de acceso a objetos • usar programas de bloqueo • acceso restringido a los equipos	• consultar registros de auditoría • copias de seguridad • revisión de las presencias en las terminales
Virus	• control sobre los programas introducidos • antivirus residente actualizado	• copias de seguridad

I.10 **DÓNDE ACTÚA LA SEGURIDAD INFORMÁTICA:** los 5 marcos de referencia



I.11 NORMAS DE APLICACIÓN:

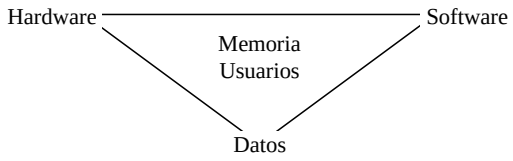
En la República Argentina sólo existen normas de Seguridad Informática para determinados tipos de empresas, además de las internas (Ej.: Comunicación "A" 2659 del BCRA); no hay leyes específicas sobre el tema, tanto a nivel nacional como provincial.
A nivel internacional se están usando las normas COBIT **(ver Anexo 3)**.

I.12 LOS 3 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA:

- Primer Principio:

  "El intruso al sistema intentará cualquier artilugio que haga más fácil su acceso y posterior ataque. El ataque siempre se realizará en el ***punto débil****".*

  El triángulo de debilidades:



  - ✓ Hardware: errores intermitentes, desconexiones, caídas, etc.
  - ✓ Software: robo de programas, modificaciones incorrectas, ejecución errónea, entropía, etc.
  - ✓ Datos: alteración de contenidos, introducción de datos falsos, manipulación fraudulenta, etc.
  - ✓ Memoria: virus, mal uso de la gestión de memoria (on - line, real - time), bloqueo del sistema (particiones FORTRAN), etc.
  - ✓ Usuarios: suplantación de identidad, acceso no autorizado (préstamo de Password), visualización de datos confidenciales, etc.

- Segundo Principio:

  "Los datos deben protegerse sólo hasta que pierdan su valor".

  Por ejemplo: históricos, tablas, etc. De no hacerse así el costo de mantenimiento y la dificultad de su administración ponen en peligro su seguridad.

- Tercer Principio:

  "Las medidas de control que se implementen deben ser efectivas, eficientes, fáciles de usar y apropiadas al medio".

  Las medidas deben funcionar en el momento oportuno, optimizando los recursos del sistema con un mínimo de molestias al usuario; de lo contrario son un gasto inútil.

I.13 RELACIÓN CON LA AUDITORÍA INFORMÁTICA:

Existe una estrecha relación entre la Auditoría Informática y la Seguridad Informática, considerándose a la primera un complemento imprescindible de la segunda, de la que a su vez extrae la mayoría de sus técnicas aplicativas.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de las organizaciones que participan en el procesamiento de la información, teniendo como fin que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

I.14 ALGUNOS CONCEPTOS FUNDAMENTALES:

- Ningún sistema de seguridad es totalmente confiable hasta que se comprueba su ***efectividad al surgir la necesidad*** de usarlo.

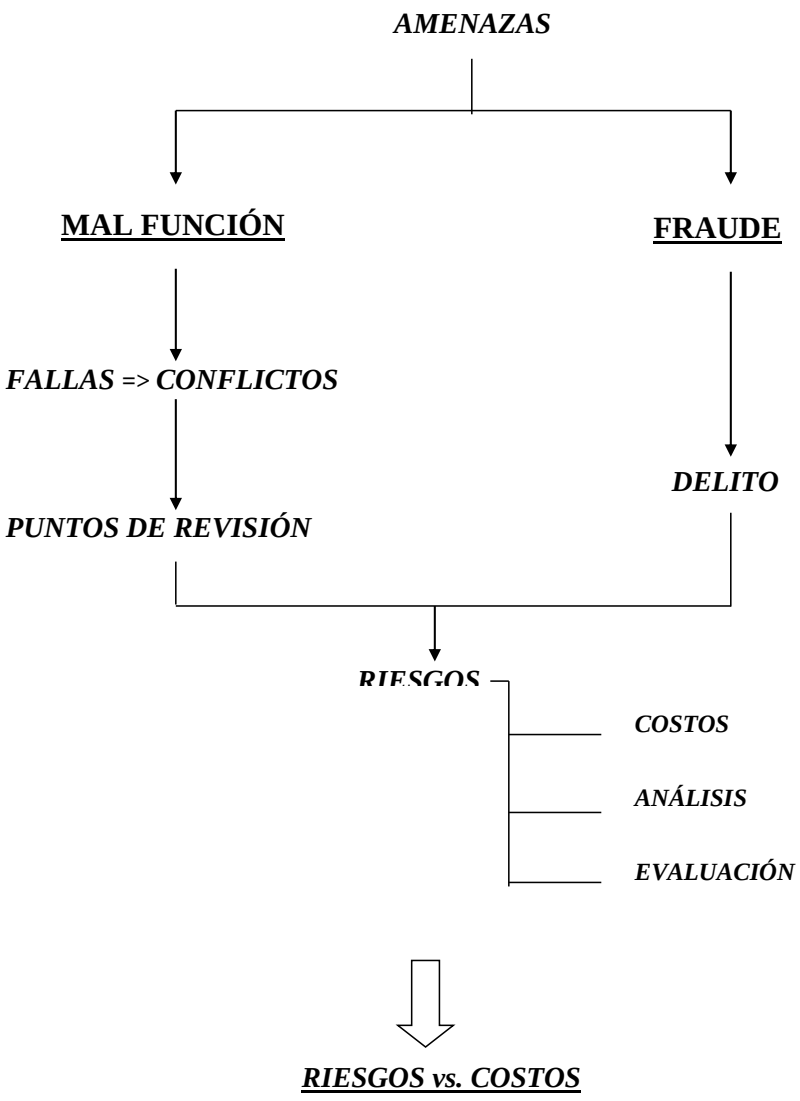
- Es imposible eliminar el riesgo. Seguridad es un concepto asociado a la certeza, riesgo o contingencia. No siendo posible la certeza absoluta, el elemento de riesgo esta siempre presente independiente de las medidas que se tomen, por lo que se debe hablar de ***niveles de seguridad***;

la seguridad absoluta no es posible y debe entenderse que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

- La seguridad Informática es un conjunto de medidas interdisciplinarias, entre las que se destacan las técnicas de control en el Diseño de Sistemas, la Criptografía y la Auditoría Informática, teniendo como objeto la custodia de los activos informáticos, fundamentalmente el principal de ellos: ***la información.***

- La Seguridad Informática es un problema integral. Sus problemas no pueden ser tratados aisladamente ya que ***la seguridad de todo el sistema es igual a la de su punto más débil.***-

II : RIESGO INFORMÁTICO



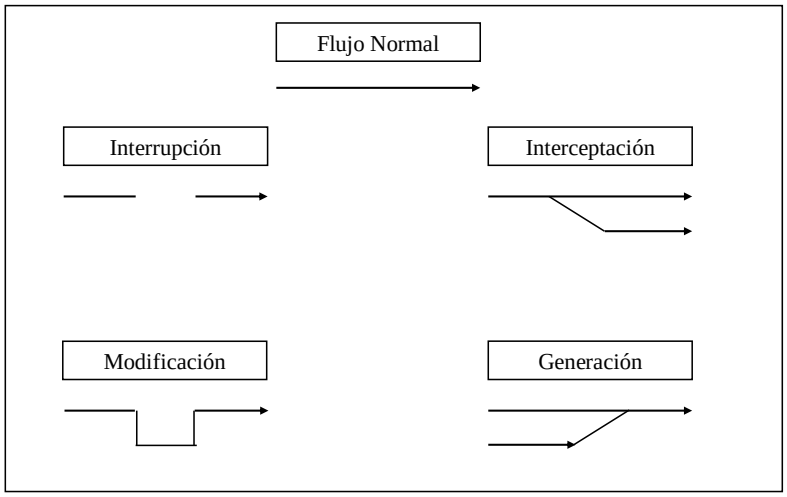
II.1 AMENAZAS, VULNERABILIDAD Y ATAQUES:

Las **amenazas** en informática determinan cuáles deben ser las orientaciones de las medidas de seguridad a adoptar. El grado de susceptibilidad y el efecto que un sistema informático tiene cuando la amenaza se convierte en realidad es la **vulnerabilidad**. La amenaza se convierte en realidad a través de un **ataque**.

De acuerdo al estado actual de la tecnología, se pueden conjugar estos tres elementos para formar una tabla orientativa.

Las amenazas afectan principalmente al Hardware, al Software y a los Datos. Estas se deben a fenómenos de:

- Interrupción
- Interceptación
- Modificación
- Generación



Estos fenómenos pueden darse por una mal función del Sistema Informático, ya sea en su diseño o explotación, o bien por hechos dolosos intencionales para producir daños al usuario o beneficios ilegales a terceros, caso en que se produce un delito.

Los **riesgos** en general no sólo están dados por la presencia de personas que perpetran los delitos sino por la ineficiencia generada por una mala administración o por un deficiente diseño y mantenimiento de los Sistemas que no consideran esta posibilidad.

II.2 EL DELITO INFORMÁTICO:

La creciente injerencia de la Informática en la Administración ha derivado hacia las áreas de Sistemas la posibilidad de delitos graves contra la propiedad y de riesgos de ineficiencia. Los principales factores que concluyen esta afirmación son:

- La conversión casi total de los procedimientos informativos manuales a procesos informáticos de todo nivel
- La dependencia que se crea del entorno tecnológico
- Los cambios permanentes en ese entorno que no permiten el dominio total de las características del hardware y software antes de que deban ser cambiados
- La interconexión en redes o equipos multitarea de usuarios de baja capacitación que dificulta el control de acceso a la información
- La reelaboración de las informaciones principales en puntos aislados (PC´s monousuarios) que pueden presentar la misma en distintas formas alterando su significación
- La vulnerabilidad de las redes públicas
- La proliferación de virus informáticos
- El alto costo de la seguridad para enfrentar un posible ilícito sin degradar las prestaciones de los sistemas

• El delito informático parece ser un "buen negocio" por:

–**Objeto Pequeño**: la información está almacenada en "contenedores pequeños": no es necesario un camión para robar el banco, joyas, dinero, etc.

–**Contacto Físico**: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del delincuente.

–**Alto Valor**: el objeto codiciado tiene un alto valor. El contenido (los datos) vale mucho más que el soporte que los almacena (disquete, disco compacto, etc.)

II.2.1 TIPIFICACIÓN DEL DELITO INFORMÁTICO:

El delito siempre tiene como objetivo los estamentos mas vulnerables. En el caso informático puede haber distintos tipos o naturalezas de delito:

- El computador como objeto de agresión: se trata de agresión física a los equipos, con finalidad variada, realizada individual o colectivamente. Puede tratarse de destrucción total o parcial de líneas, equipos centrales, terminales, etc. con fines vandálicos, intimidatorios o de venganza; también con fin de robo de componentes, aunque no es muy frecuente por la posterior dificultad de su comercialización.

- El computador como generador de un entorno especial: Aquí se usa el computador para la creación de un entorno único que en el cual resulten posibles acciones delictivas, cuando se crean activos que posteriormente pueden ser sujetos de acciones delictivas, caso archivos con información sensible expuestos a accesos no autorizados.

- Empleo del computador como instrumento del delito: Se usa el computador para cometer una acción ilícita (alteración de programas, cambio de saldos en archivos, desvío de fondos, anulación de facturas, etc.).

- Uso del computador para defraudar a las víctimas: basado en la dificultad del usuario no especializado para comprobar la mal función, el computador se usa como excusa para la defraudación. Ejemplo, caso agencia de cobranzas que sobrefactura o cobra importes mayores, imputando el error al Sistema..

- El robo de propiedad intelectual: Fundamentalmente software de aplicación; la dificultad de prevención de copias y la falta de legislación adecuada hace casi imposible el control de estos delitos.

- El daño por virus informáticos: Afecta a la propiedad fisica e intelectual.

- La entrada no autorizada a redes: Tanto LAN como MAN, WAN o Internet; uso de los productos o informaciones sin autorización o alteraciones en los contenidos de los mensajes.

II.2.2 PERFIL DEL DELINCUENTE INFORMÁTICO:

Dado que los delitos que se cometen son nuevos, su perfil también lo es. En general tienen las siguientes características:

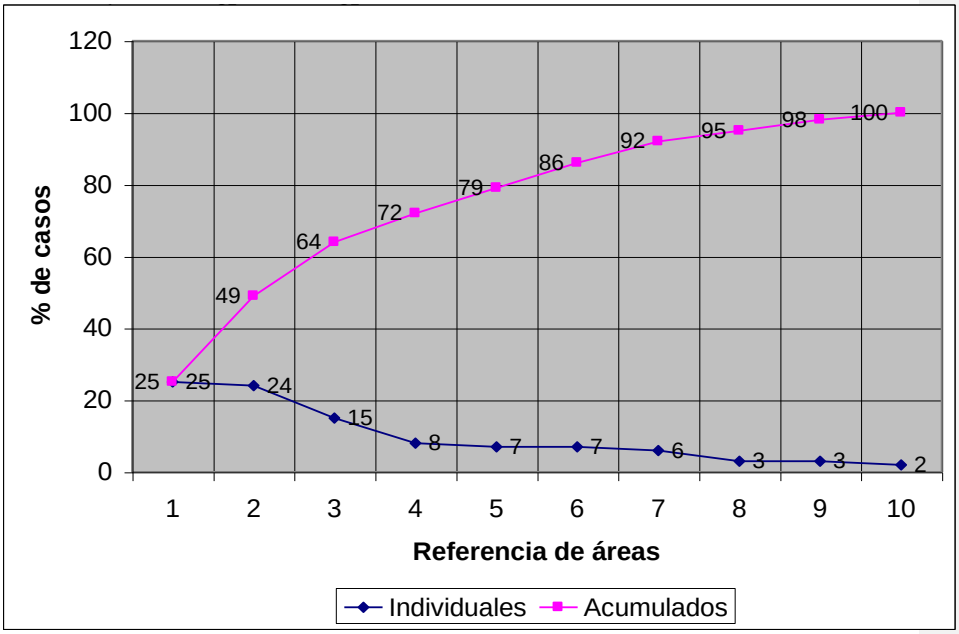
- No tienen antecedentes delictivos previos en otros rubros
- En su gran mayoría son varones; las mujeres se encuentran implicadas sólo a nivel de complicidad
- El rango de edad está entre los 18 y 30 años
- Pocas veces actúan en asociación, suele haber un solo ejecutor y a lo sumo una o dos personas de apoyo
- Todos tienen un conocimiento altamente especializado
- Suelen comenzar como un desafio a los límites que pone el computador para su acceso y luego derivan al delito económico

II.2.3 ÁREAS MÁS VULNERADAS POR EL DELITO INFORMÁTICO:

Según estadísticas de EEUU, los delitos informáticos agrupados por tipo representan los siguientes porcentajes:

1. Acceso fisico a los recursos: 25%
2. Manejo de la información de entrada: 24%
3. Acceso lógico a los archivos: 15%
4. Manejo de la información de salida: 8%
5. Acceso a los programas de aplicación: 7%
6. Manejo de la información contenida en medios legibles: 7%

7. Infracción a la ética comercial: 6%
8. Acceso a los programas del sistema operativo: 3%
9. Alteración de resguardos y recuperación: 3%
10. Ataques a transmisión de datos y redes: 2%



Se puede observar que las 3 primeras causas representan los dos tercios de los delitos y están dados en áreas de control interno del área de Sistemas, que son las que menos conocimiento técnico requieren para el ataque, por lo cual es en ellas donde deben volcarse primariamente los esfuerzos.

II.2.4 FORMAS MÁS COMUNES DEL DELITO INFORMÁTICO:

Sin excluir una variedad de modalidades nuevas que constantemente aparecen, las de mayor influencia se basan en los mismos métodos; en general son sencillos de prevenir y detectar si se tiene en cuenta su posible existencia; su dificultad de prevención se acrecienta cuando se usan combinados o con pistas falsas:

- Adulteración de la información de entrada: Es el medio más simple y más usado. Muchas veces no hace falta que se tomen medidas para eliminar el fraude posteriormente, puesto que el ciclo de comprobación de la información es mayor que el necesario para cometer el ilícito. Es conveniente, ya que con esta consideración se agregan a los posibles perpetradores personas que no tienen un alto conocimiento de Informática, agregar controles sorpresivos a las validaciones corrientes o bien reducir drásticamente los periodos de cruce de la información de entrada con los resultados.

- Técnica del "Caballo de Troya": Significa tener uno o más programas con una "puerta trampa", que se abre bajo determinadas condiciones que benefician al perpetrador (un legajo, una fecha, algún código de cliente, determinado número de cuenta, etc.). Suele incluir técnicas de desvanecimiento de los datos alterados, basadas en general en deficiencias de diseño del Sistema, si se usa más de una vez. Sólo puede ser usado por personal de alta especialización y gran conocimiento del Sistema.

- Técnica del salchichón: Se trata de obtener fracciones de difícil control, como por ejemplo centavos de redondeo, en operaciones muy numerosas. También se usa para el desvanecimiento para los resultados producidos por las técnicas anteriores. El delincuente debe tener las mismas condiciones que el anterior.

II.2.5 FRAUDES:

Específicamente se pueden clasificar los fraudes que se cometen en los sistemas informáticos, o sea las acciones que conducen al delito y, consecuentemente, al perjuicio económico de alguien por quien perpetra el fraude. Los más comunes son:

- Manipulación indebida, falsificación o alteración de registros y documentos

- Supresión u omisión de los efectos de la transacción en los registros o documentos

- Registración de transacciones inexistentes

- Uso indebido de las políticas contables
- Malversación de los activos

II.2.6 CONDICIONES QUE AUMENTAN EL RIESGO DE FRAUDE:

Implica los contextos que facilitan la comisión del fraude, o sea condiciones inadecuadas para el desenvolvimiento de las tareas informáticas:

- Administración controlada por una o pocas personas sin supervisión gerencial
- Estructura organizacional compleja, sin clara definición de autoridad y responsabilidad
- Deficiencias importantes en el control interno
- Alta rotación del personal clave
- Plantel insuficiente durante períodos prolongados
- Cambios de auditores frecuentes
- Actividad de la empresa cambiante (aumenta o decrece rápidamente) que implica aumento de las fallas
- Inestabilidad del mercado
- Dificultades financieras (en achicamiento o expansión)
- Operaciones sin autorización formal
- Archivos sujetos a ajustes frecuentes, operaciones no contabilizadas o no conciliadas
- Documentación insuficiente o desactualizada de programas y sistemas
- Cambios frecuentes de programas, sin documentar, autorizar y probar
- Existencia de puntos débiles para acceder al sistema

- Falta de destrucción adecuada de la información en desuso (listados, carbónicos, etc.)
- Personal de Sistemas es especialmente sensible a la presión o extorsión
- Sistemas Operativos con bajos niveles de Seguridad
- Métodos criptográficos accesibles o insuficientemente aplicados

II.2.7 DIFICULTAD PARA DETECTAR FRAUDES:

Son más difíciles de detectar cuando:

- Son varias las personas involucradas
- Se planifica a alto nivel
- Los controles relacionados son débiles
- Existe la posibilidad de venta de datos o software a terceros
- No se someten a auditorías especializadas

II.3 FALLAS MAS COMUNES POR FUNCIÓN INADECUADA EN EL AMBIENTE INFORMÁTICO:

Agrupa los posibles ***conflictos*** que pueden presentarse a partir de un ***funcionamiento inadecuado del área informática***, que repercute en distintos sectores de la empresa:

II.3.1 PROPIOS DE LA ACTIVIDAD DE LA EMPRESA:

- Pérdida de mercado
- Errores en el manejo financiero
- Caída de la eficiencia operativa
- Pérdida de activos

II.3.2 EN LA CAPTURA E INGRESO DE DATOS:

- Errores y omisiones (casuales o maliciosos)
- Pérdidas, alteraciones, agregados y supresiones
- Violación de la privacidad
- Falsedad ideológica
- Inconsistencias no detectadas

II.3.3 EN EL DESARROLLO DE SISTEMAS:

- Decisión estratégica equivocada al decidir el sistema, su metodología de desarrollo, su modalidad de contrato o el proveedor
- Factibilidad imprecisa o errónea
- No cumplimiento de objetivos por definición imprecisa o relevamiento incompleto
- Inadecuada selección de equipos y software de base
- Falta de seguridad en los resultados por pruebas superficiales o incompletas
- Baja confiabilidad del software terminado ante contingencias operativas por falta de previsión de las mismas
- Demoras excesivas en los tiempos de desarrollo que aumentan la entropía
- Sustracción de filosofia del sistema, programas o técnicas de medios
- Falta de planificación, control de calidad y avance del proyecto que produce incompatibilidad con otros sistemas en operación o desarrollo
- Problemas de mantenimiento por fallas en la Documentación
- Falla en los controles automáticos por falta de integración o carencia de pistas de auditoría

II.3.4 EN EL PROCESAMIENTO DE DATOS:

- Pérdida de datos por fallas de hardware, software o sistemas de resguardo y recuperación
- Degradación de la operación por fallas del Sistema
- Recuperación de datos incompletos o erróneos por fallas en los dispositivos de comunicaciones
- Exposición a accidentes o daños por fenómenos naturales que no se preveen
- Vandalismo, sabotaje y ataques por virus
- Demoras excesivas en obtener resultados de los procesos
- Riesgos de System Crash por operación sobre equipos cercanos al nivel de saturación
- Riesgo de discontinuidad por falta de redundancia
- Usos de los equipamientos para operaciones externas a la empresa o no autorizadas
- Daño o deterioro de los recursos y medios magnéticos
- Falencias en la destrucción programada de documentación sensible
- Robos de medios, dispositivos, archivos y bibliotecas por falta de protección
- Violación de privacidad y confidencialidad de los datos procesados

II.3.5 EN EL ÁREA USUARIA:

- Resultados del Procesamiento que no satisfacen a los usuarios

- Fallas en el control por Auditoría Operativa esporádica y/o parcial, revisiones inconsistentes con los resultados de los procesos
- Falta de correlación entre los datos ingresados y los resultados obtenidos por errores de diseño
- Demoras, mala conservación, mal uso, pérdidas o deterioro de la información procesada
- Falta de confidencialidad en el manejo de datos sensibles
- Uso de claves de otros usuarios o uso negligente de las claves propias
- Falta de procedimientos manuales para contingencias
- Inseguridad en los datos por uso de programas para PC´s no depurados (virus) o no autorizados
- Inadecuado control y protección de medios magnéticos o archivos a su cargo
- Copiado de programas de la empresa para uso propio o de terceros
- Baja capacitación del personal, ocasionada por alta rotación, bajo entrenamiento o actitud hostil
- Falta de oportunidad de uso de la información por archivado caótico o irregular

II.3.6 EN LA RELACIÓN CON ÁREAS EXTERNAS O PROVEEDORES:

- Desprotección contractual por contratos de adhesión, cláusulas leoninas, falta de especificaciones para incumplimiento y zonas grises de conflicto
- Problemas de mantenimiento por carencia de soporte, servicio, reticencia a la entrega de programas fuente y dudosa continuidad operativa del proveedor
- Riesgo en la confiabilidad por procesamientos o uso de bibliotecas compartidas con otros clientes

- Niveles de seguridad más bajos que los de la empresa contratante
- Interpretación inadecuada de los requerimientos de la empresa contratante
- Demoras o atrasos en otros proyectos ligados al contratado
- Posibilidad de robo o abuso de información u otros activos del contratante

II.3.7 EN LA RELACIÓN CON ENTES EXTERNOS:

- Débitos y créditos directos
- Correo electrónico (vía MODEM, Internet o Intranet)
- Uso de ATM´s (Automatic Treller Machine)
- Declaraciones y pagos de impuestos
- Compras y pagos con "dinero plástico"

II.4 PUNTOS DE REVISIÓN MAS COMUNES EN SEGURIDAD INFORMÁTICA:

Para realizar la verificación de los controles implementados y determinar si existen riesgos en las áreas específicas se deben observar los siguientes **puntos de revisión**:

1. Administración de la seguridad
2. Criptografía
3. Control de acceso a datos, lógico y físico
4. Seguridad en la Operación de los Sistemas (documentación, control de acceso, capacitación de operadores, etc.)

5. Seguridad en Sistemas de oficina: en el uso de los utilitarios en puestos descentralizados, autorización para programas especiales, uso de paquetes, etc., con comparación de resultados con los Sistemas

6. Protección de instalaciones, principales y auxiliares

7. Controles sobre las Bases de Datos:

   - accesibilidad de los utilitarios,
   - manejo del administrador
   - autorización para el uso de programas y paquetes
   - uso de los administradores de dispositivos
   - capacidades de los querys y posibilidades de modificación con programas externos

8. Seguridad en las redes de comunicaciones:

   - redundancia
   - protección de accesos no autorizados
   - velocidades aceptables
   - estadísticas de fallas

9. Seguridad en el desarrollo de Sistemas:

   - acceso a datos reales
   - manejo de las bases de prueba
   - documentación y dominio de metodologías y lenguajes por parte del personal

10. Mantenimiento de equipos y Sistemas:

    - contratos de mantenimiento

- estadísticas de fallas y respuestas
- tiempos de parada debido a fallas para determinar la posibilidad de obsolescencia y seguridad en las actividades de los mantenedores

11. Métodos de prueba de los Sistemas:

- en la implementación y en el mantenimiento
- verificación de la existencia de lotes y su actualización
- frecuencia de comprobación en producción y cobertura de las pruebas

12. Procedimientos de cambios a programas:

- uso de bibliotecas intermedias
- comprobación con lotes de prueba
- verificación del nivel de autorización
- control de versiones
- autorización de las modificaciones respecto al Plan de Sistemas
- relaciones con archivos históricos

13. Personal:

- profesionalidad
- fidelidad
- permanencia
- control de ingresos y egresos monetarios
- existencia de un sistema de calificación periódico
- actitud frente a los cambios
- nivel de rotación y causas de la misma

II.5 EVALUACIÓN DE RIESGOS:

El siguiente es un método para elaborar tablas de valuación de los riesgos ya descriptos; es empírico, pudiendo darse otros de acuerdo a la evolución tecnológica de las aplicaciones, hardware, estado de las comunicaciones, etc., de manera que el presente sirve como base de construcción pero no es excluyente de otros métodos o valores de clasificación.

II.5.1 MÉTODO DE EVALUACIÓN POR PONDERACIÓN:

Para evaluar un riesgo siempre deben considerarse dos factores: la probabilidad de ocurrencia y la severidad de la pérdida si ésta ocurre. Los ***pasos para preparar una evaluación de riesgo*** son:

1. Identificar todas las áreas cuyo riesgo tiene que ser evaluado

2. Obtener un buen conocimiento de las actividades desarrolladas en cada área, sus objetivos y responsabilidades

3. Considerar la característica de cada riesgo analizado de acuerdo a las tablas desarrolladas más abajo

4. De ser posible, promediar los valores de los riesgos calificados tomando evaluaciones individuales de distintos miembros del equipo obteniendo un índice de ponderación para cada uno, usando por ejemplo:

Índice de ponderación = Puntaje medio del evento / Puntaje Individual

Valor Corregido = Valor Original * Índice Ponderación

Por ejemplo:

	VALORES ORIGINALES					VALORES CORREGIDOS		
Evaluador	Evento 1	Evento 2	Evento 3	Promedio Evaluador	Índice de Ponderación	Evento 1	Evento 2	Evento 3
A	6,0000	8,1000	5,5000	6,5333	1,0459	6,2755	8,4719	5,7526
B	9,5000	9,8000	7,9000	9,0667	0,7537	7,1599	7,3860	5,9540
C	5,2000	6,0000	3,5000	4,9000	1,3946	7,2517	8,3673	4,8810
Media	6,9000	7,9667	5,6333	6,8333		6,8957	8,0751	5,5292
					Corrección %	0,0621	-1,3612	1,8488

5. Calcular el Puntaje Total y clasificarlo en orden descendente de importancia relativa: >=100, alto riesgo; de 99 a 70, mediano riesgo y <70 bajo riesgo

El Total es la suma de los valores individuales y representa la calificación asignada al riesgo. Las características son evaluadas de 0 a 10 para indicar el grado de importancia relativa asignada en cada caso. Estas características del riesgo se detallan a continuación dando las pautas a considerar para cada clasificación:

1. Impacto sobre activos, pasivos y flujos de caja: se considerará el riesgo de impacto tanto en los negocios de la Empresa como en los de sus clientes si los sistemas aplicativos funciona incorrectamente, fallan los controles clave, hay fraude, errores o no puede funcionar por períodos prolongados (se consideran mayores al lapso de cierre de operaciones de la Empresa):

    - de 1$ a 1.000.000$ → 0-3
    - de 1.000.000$ a 3.000.000$ → 4-7
    - + de 3.000.000$ → 8-10

2. Valuación de los datos: se evalúan los datos en función de su sensibilidad:

    - Altamente confidencial (su difusión pone en riesgo la existencia de la organización) → 10
    - Confidencial (su difusión crea un daño económico variable) → 6-9
    - Interno (su difusión no crea daño económico directo, pero si problemas operativos) → 1-5
    - Público → 0

3. Evaluación del riesgo de pérdida de los datos: evaluando los métodos de transporte, ingreso y conservación de los datos:

    - Alto riesgo de pérdida (prácticamente existe la seguridad que la pérdida se producirá) → 10

- Mediano riesgo (los sistemas no dan seguridades, normalmente se basan sólo en la habilidad y confiabilidad de los operadores) → 6-9
- Bajo riesgo (seguridad casi absoluta, sólo una catástrofe puede ocasionar pérdidas): → 0-5

4. Complejidad de la operativa: basándose en el principio que los sistemas complejos son frágiles y mas vulnerables a fallas, interrupciones y brechas en la seguridad que otros más simples, se analizan las principales áreas de riesgo de los procesos, como ser: sistemas distribuidos, sistemas complejos de archivos y bases de datos, redes extensas y sus sistemas de comunicación y grandes sistemas en tiempo real integrados. La escala será:

   - Alta complejidad (muchas operaciones diferentes con gran interrelación entre las partes componentes) → 8-10
   - Complejidad Media (variedad de operaciones con alguna interrelación) → 4-7
   - Baja Complejidad (ingreso de datos simple, procesamiento mayoritariamente batch, salidas con poca relación entre sí, poca dependencia de otros sistemas): → 0-3

5. Gestión Gerencial: se considera la calidad del ambiente gerencial, si existen políticas, estrategias y planes definidos, buena organización, experiencia y entrenamiento del personal bien planificado, historial relevante de trabajos anteriores, relación éxitos / fracasos, comunicación entre usuarios y proveedores de Información Tecnológica, etc.:

   - Mala gestión (Carencia de políticas y estrategias de negocios, organización pobre, prácticas de trabajo pobres o no formuladas, poca experiencia previa, poca conexión usuarios / sistemas, antecedentes dudosos) → 8-10
   - Gestión regular (Estructura básica gerencial con roles definidos, prácticas de trabajo definidas, alguna conexión entre usuarios / sistemas) → 4-7
   - Buena gestión (prácticas de trabajo bien desarrolladas y utilizadas con un alto nivel de participación del usuario, historial exitoso y equipo gerencial maduro y efectivo) → 0-3

6. Personal: Rotación, tasas de ausentismo por distintas razones, nivel de experiencia, calidad de entrenamiento, nivel de relaciones personal -gerencia, moral colectiva:

   - Personal ineficiente (alta rotación, escasa experiencia, baja moral y pobres relaciones con la Gerencia) → 8-10
   - Personal medio (problemas en dos áreas como máximo de las arriba mencionadas) → 4-7
   - Personal eficiente (personal altamente motivado y experimentado, sin ninguna de los problemas mencionados) → 0-3

7. Estabilidad: Las áreas de negocios que están poco sujetas a cambios están poco expuestas a errores. Los aspectos de la estabilidad incluyen: frecuencia de cambios debidos a requerimientos normativos, de negocios o de fallas inherentes al sistema utilizado; frecuencia de cambios urgentes a sistemas; cantidad de mejoras pedidas al sistema y cantidad de áreas de negocios con las que se conecta el sistema. Si un sistema es desconocido se le asigna un puntaje de 6, de otra forma se aplica:

   - Alto grado de inestabilidad → 8-10
   - Estabilidad promedio o desconocida → 4-7
   - Ambiente muy estable → 0-3

8. Implicancias de carácter legal y regulatorio: las actividades de la Empresa que están sujetas a responsabilidades adicionales, mas allá de las inherentes a la operación con sus clientes, tales como organismos impositivos, Aduanas, Banco Central, Comisión de Valores, etc.. El incumplimiento con estas entidades puede tener graves consecuencias en la Empresa, por lo que se evalúa en que medida está afectada su actividad por las regulaciones que imponen estos organismos externos:

   - Alta influencia (el sistema externo controla la principal línea de actividad comercial o tiene serias implicancias legales para la Empresa si ocurren fallas) → 10
   - Influencia media (el sistema externo controla una línea actividad importante de la Empresa y puede tener implicaciones legales importantes) → 5-9
   - Baja influencia (el sistema externo controla una línea comercial secundaria y requiere informes periódicos) → 1-4

- Ninguna influencia (la Empresa no debe responder a ningún sistema externo) → 0

Con estos puntajes se construye una matriz como la siguiente:

	PUNTAJE											
Factores	0	1	2	3	4	5	6	7	8	9	10	Clasif.
a) Act./Pas. / Flujo de caja	$1	$10K	$100k	$1M	$1,5M	$2M	$2,5M	$3M	$3,5M	$4M	>4M	
b) Valuación datos	Público	Interno	Interno	Interno	Interno	Interno	Conf	Conf	Conf	Conf	Muy conf.	
c) Riesgos datos	...											
d) Complejidad												
e) Gestión Gerencial												
f) Personal												
g) Estabilidad												
h) Legal/ normas												
										TOTAL		

II.5.2 MÉTODO DE EXPECTATIVA ANUAL DE PÉRDIDAS (EAP):

Se hacen dos estimaciones:

- Impacto**:** pérdida en términos monetarios que ocasionaría la pérdida de un determinado hecho
- Frecuencia: probabilidad que ocurra el hecho una vez cada cierto tiempo

PÉRDIDA = IMPACTO * FRECUENCIA

Las estimaciones más comunes en la práctica para Impacto (i) y Frecuencia (f) son:

- $10 → i=1
- $100 → i=2
- $1K → i=3
- $10K → i=4
- $100K → i=5
- $1M → i=6
- $10M → i=7
- $100M → i=8

- 300 años → f = 1
- 30 años → f = 2
- 3 años → f = 3
- 100 días → f = 4
- 10 días → f = 5
- 1 día → f = 6
- 10 veces / día → f = 7
- 100 veces / día → f = 8

EAP= (10 ** (F + I - 3)) / 3

Por ejemplo, si sucede una vez cada 3 años y la pérdida es de 10.000$:

EAP = (10*(3+4-3)) / 3 = 10000/3 = 3.000$

En el ***Anexo 1*** se desarrollan los temas clásicos para evaluar los principales temas de Seguridad Informática y poder aplicar estos métodos.

II.6 MATRIZ DE ANÁLISIS DE RIESGOS:

Se usa para identificar y cuantificar los riesgos y así determinar los puntos más sensibles donde aplicar la Seguridad Informática.

En la Matriz de Análisis se colocan en las filas los distintos elementos sobre los que puede actuar el riesgo y en las columnas el riesgo en sí a que pueden ser sometidos. En las celdas se cuantifican de acuerdo a alguno de los métodos vistos u otros que permitan dar magnitudes a los valores de riesgo.

Una vez completados, se aplica uno de los métodos de evaluación y se obtienen los valores monetarios del riesgo, los que luego servirán para cotejar con el costo de los controles a implementar para eliminarlos.

En el ejemplo se utiliza el método de Expectativa Anual de Pérdida.

M A T R I Z D E A N Á L I S I S R I E S G O S

AMENAZAS / COMPONENTES	DESTRUCCIÓN INTERRUPCIÓN DEL SERVICIO	ACCESO FÍSICO / LÓGICO NO AUTORIZADO	ALTERACIONES	ERRORES OMISIONES	COSTOS EXCESIVOS	FRAUDE O ROBO	FALLAS FUNCIONAMIENTO	CONTRAVENCIONES	DIVULGACIÓN NO AUTORIZADA
INFORMACIÓN									
EQUIPOS									
PROGRAMAS									
REDES									
OPERACIONES									
FACILIDADES									
RECUPERO DESASTRES									

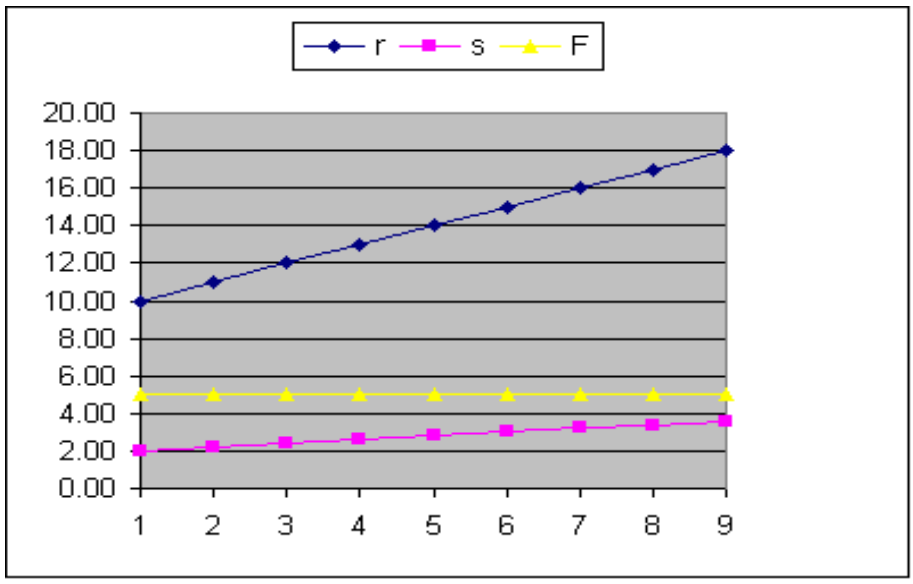
M A T R I Z D E E V A L U A C I Ó N D E R I E S G O S

Frecuencia		Una vez cada 300 años	Una vez cada 30 años	Una vez cada 3 años	Una vez Cada 100 días	Una vez cada 10 días	Una vez por día	10 veces por día	100 veces por día
Impacto	f. / i.	1	2	3	4	5	6	7	8
$ 10	1	—	—	—	—	$ 300	$ 3 K	$ 30 K	$ 300 K
$ 100	2	—	—	—	$ 300	$ 3 K	$ 30 K	$ 300 K	3 M
$ 1,000	3	—	—	$ 300	$ 3 K	$ 30 K	$ 300 K	3 M	30 M
$ 10,000	4	—	$ 300	$ 3 K	$ 30 K	$ 300 K	3 M	30 M	300 M
$ 100,000	5	$ 300	$ 3 K	$ 30 K	$ 300 K	3 M	30 M	300 M	—
$ 1,000,000	6	$ 3 K	$ 30 K	$ 300 K	3 M	30 M	300 M	—	—
$ 10,000,000	7	$ 30 K	$ 300 K	3 M	30 M	300 M	—	—	—
$100,000,000	8	$ 300 K	3 M	30 M	300 M	—	—	—	—
		E X P E C T A T I V A A N U A L D E P É R D I D A							

II.7 RIESGOS vs. COSTOS:

Tomando el riesgo como la probabilidad que se materialice una amenaza, los valores económicos de los riesgos a correr son inversamente proporcionales al gasto en Seguridad Informática:

$$\text{Factor de riesgo} = \frac{\text{r (costo del riesgo)}}{\text{s (gasto en seguridad)}}$$



	r	s	F
1	10,00	2,00	5,00
2	11,00	2,20	5,00
3	12,00	2,40	5,00
4	13,00	2,60	5,00
5	14,00	2,80	5,00
6	15,00	3,00	5,00
7	16,00	3,20	5,00
8	17,00	3,40	5,00
9	18,00	3,60	5,00

El valor *r / s* varía con la tecnología que se aplique, por lo tanto el nivel del Factor de Riesgo lo decide la Gerencia en base a la política de Seguridad de la organización.

El valor de *s* se toma con un nivel de seguridad 1 que el riesgo correspondiente *r* sea anulado; por ello, para mantener el valor de *F* constante, el valor de *s* debe aumentarse proporcionalmente a medida que la pérdida que implica el riesgo asociado aumenta.-

III : SEGURIDAD FÍSICA EN INSTALACIONES

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de la emergencia hasta que sea restaurado el servicio completo.

III.1 Seguridad contra incendios

Uno de los principales riesgos de los centros de cómputos son los incendios, por la acumulación de materiales inflamables (papeles, plásticos, revestimientos, etc.) y el riesgo de combustión por chispas dado el uso de equipos eléctricos y la baja humedad que debe reinar en el ambiente acondicionado.

Entre las precauciones que se deben revisar están:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.

- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.

- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Esto es común en lugares donde se encuentran trabajando personas de distinta capacidad física y los extintores están a tal altura o con un peso tan grande que no todos pueden utilizarlos.

- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.

- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.

- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

A este respecto, se pueden revisar los cuestionarios de Seguridad Física del **Anexo 1** y el punto G, Matriz de control de Seguridad Física del **Anexo 2** por el método de Fitzgerald.

Los elementos mas importantes a utilizar son:

- Detectores: se deben combinar de dos tipos: térmicos, que detectan en base a bimetales aumentos de temperatura actuando cuando se supera un cierto límite, y de humo en base a la interferencia del mismo en una cámara de descarga radiactiva sobre una célula sensible.

- Extintores: manuales: capacidad, facilidad de acceso, peso y tipo de producto; automáticos: CO_2, freón, halón (peligrosos si no se desaloja).

- Entrenamiento del personal: rol de cada uno ante el siniestro – responsable de cada etapa.

- Marcaciones de salida.

- Vigilancia permanente.

- Protección ignífuga de almacenamientos externos.

- Duchas salvavidas.

- Salidas de emergencia, mínimo una además de las normales, vigilando que sean accesible a personas de cualquier condición física.

III.2 Seguridad de Acceso Físico:

Dado que la mayoría de los ataques a la Seguridad se producen en áreas de complejidad simples, como las de entrada / salida e ingreso de datos, es importante que los ingresos físicos de personas estén altamente controlados.

III.2.1 Métodos biométricos:

En el ámbito de las tecnologías de la seguridad, uno de los problemas fundamentales a solventar es la necesidad de autenticar de forma segura la identidad de las personas que pretenden acceder a un determinado servicio o recinto físico. De este modo, surge la biometría, también conocida como técnicas de identificación biométrica, con el objetivo de resolver este problema a partir de características que son propias de cada individuo, como voz, huella dactilar, rostro, etc.

Estas técnicas de identificación biométricas, frente a otras formas de autenticación personal como el uso de tarjetas o PINes (Personal Identification Number, o número de identificación personal, como el usado en cajeros automáticos), tienen la ventaja de que los patrones no pueden perderse o ser sustraídos, ni pueden ser usados por otros individuos en el caso de que lleguen a tener accesible nuestra tarjeta personal y/o PIN.

Debemos tener en cuenta que gran parte de los sistemas de autenticación actuales están basados únicamente en el uso de una tarjeta personal y/o PIN. Así, por ejemplo, es habitual que en el caso de pérdida o sustracción de una cartera cualquiera pueda hacerse pasar por uno mismo, ya que es extremadamente frecuente tener junto a las tarjetas personales, el / los número / s secretos (PINes) apuntado / s en la misma. Éste problema de suplantación de identidad quedaría totalmente resuelto con el uso de patrones biométricos como medio de autenticación personal, debido a que dependen de características físicas del autorizado que no pueden ser sustraídas o remplazadas.

Todo método biométrico tiene 4 pasos:

1. Captar la característica física del usuario

2. Modificar los datos en bruto captados y digitalizarlos para extraer los parámetros básicos, eliminando las condiciones externas a la medición

3. Comparar los datos obtenidos con los almacenados

4. Accionar sobre el sistema de acceso, franqueándolo si los datos se corresponden o emitiendo una alarma en caso contrario

III.2.1.1 Técnicas de autenticación biométricas más extendidas y aplicables:

Se las describe en términos de:
- P: precisión
- C: costo
- A: aceptación por parte del usuario
- I: grado de intrusión

La técnica ideal tendría Precisión y Aceptación máximas, y Costo e Intrusión mínimas:
- P + + + +
- C +
- A + + + +
- I +

De este modo podemos enumerar:

- Reconocimiento de Huella dactilar: el usuario sólo tiene que situar la yema de un dedo (normalmente el índice) sobre un escáner de huella.

  Evaluación:
  - P + + + +
  - C + +
  - A + + +
  - I + +

- Reconocimiento Facial: el sistema dispone de una cámara que graba al usuario, analizando el rostro del individuo.

  Evaluación:
  - P + +
  - C + + +
  - A + +
  - I +

- Temperatura corporal: mide la temperatura del cuerpo en distintas zonas por sensores térmicos y las compara, dando un mapa de calor o termograma. Se usan sensores en una placa que no tiene contacto con el individuo.

  Evaluación:
  - P + +
  - C + + + +
  - A + + +
  - I +

- Reconocimiento de voz*:* la persona pronuncia un código de acceso prefijado (nombre y/o apellidos, DNI, número de teléfono, PIN, etc.), o una frase diferente cada vez por invitación del sistema (diga usted...), siendo reconocido por el sistema a partir de las características de la voz grabada en el momento del acceso.

  Evaluación:
  - P + + +
  - C +
  - A + +
  - I +

- Reconocimiento de la forma de la mano: la persona sitúa su mano abierta sobre un escáner específico, siendo reconocido a partir de la forma y geometría de la misma.

  Evaluación:
  - P + +
  - C + + +
  - A + +
  - I + +

- Reconocimiento del iris: el sistema obtiene una imagen precisa del patrón de iris del individuo, evaluando los círculos concéntricos que lo forman y lo compara con el patrón previamente guardado del usuario.

  Evaluación:
  - P + + + +
  - C + + + +
  - A + + +
  - I + + +

Sin embargo, sea cual sea la técnica seleccionada para una determinada aplicación, tendremos que ponderar en cada caso las restricciones o peculiaridades que pueden tener cada una de las técnicas, frente al grado de seguridad añadido que conseguimos y

del que anteriormente no disponíamos. Estas características a ponderar vienen dadas básicamente por los siguientes aspectos:

- ✓ Necesidad de un dispositivo de adquisición específico (lector de huella dactilar, micrófono, cámara, etc.) allí donde esté el usuario.
- ✓ Posible variabilidad con el tiempo del patrón a identificar (afonías ó catarros en voz, uso de gafas/ bigote/ barba/ etc. en rostro, etc.).
- ✓ Probabilidad de error individual de cada una de las técnicas (entre uno por cien y uno entre varios millones, en función de la técnica elegida).
- ✓ Aceptación por parte del usuario de cada una de las técnicas, en función de si son o no técnicas intrusivas, cómodas, que mantengan (o al menos lo parezca) la privacidad, sencillas de usar, etc.

III.2.2 Otros Métodos de Control de Acceso Físico:

- Tarjeta magnética (perforada)
- Tarjeta con chip
- Tarjeta UHF
- Códigos de barras
- Reconocimiento de firma
- Passwords por teclado
- Detector de metales
- Detectores de sustancias

III.3 Seguridad en el lay - out de los Centros de Cómputo:

- Espacial: no sótanos ni pisos altos, construcciones antisísmicas; fuera de la vista, lejos de UHF y VHF.
- Materiales: no inflamables, no utilizar vidrios
- AA, equipos redundantes, agua para torres, limpieza de ductos, filtros
- Piso, techo
- Alarmas: ubicación, conexiones, interruptores
- Muebles metálicos
- Salida de emergencia
- Acceso único
- Cintoteca anexa

III.4 Seguridad de acceso y transporte de documentación base:

Para aquellos casos donde la documentación base deba ser trasladada para ser grabada en el centro de cómputo, se deben tener medidas de seguridad informática desde el envío, el traslado, el uso y la devolución (o destrucción o archivo):

- Envío: en bolsas selladas y numeradas, con remito, agrupadas en lotes con cabeza que contengan como mínimo: tipo de documento, el total de documentos y el total de una cifra que sea común a todos.

- Traslado: con alto nivel de seguridad, tanto en el acceso como en la protección contra accidentes.

- Uso: deben existir registros que contengan: cantidades, enumeración y procedencia de las bolsas, los lotes, con las características de cabeza, a quién se le entrega los lotes, y se emita un listado al final de proceso que verifique que se ingresó el total de los documentos, que los totales de lotes coinciden, cuáles registros fueron aceptados y cuáles rechazados.

- Devolución: si se reenvía, debe hacerse con los lotes reenumerados y los listados de control; si se guarda en el centro de cómputo se hace de la misma forma y si se destruyen los documentos los listados de control deben guardarse por el tiempo que determine la Seguridad Informática.

III.5 Protección contra agresiones:

Guardias de seguridad, alarmas, rejas, puertas, techos, etc. permanentes. La agresión puede ser por vandalismo, terrorismo, competencia desleal, empleados disgustados o sabotaje de marcas.

III.6 Protección contra desastres naturales:

- Inundación: se evita por la ubicación física (no en sótanos).
- Terremotos: construcciones antisísmicas
- Tormentas eléctricas: descarga a torres, pararrayos, corrientes residuales (fusibles gaseosos, térmicos, disyuntores)
- Vientos fuertes: tensores de las antenas

III.7 Abastecimiento de electricidad:

Se deben contemplar dos principios:

- Abastecimiento ininterrumpido: UPS
- Fuente permanente de emergencia: líneas alternativas o grupos generadores (tener en cuenta el combustible).

III.7.1 Capacidad de UPS necesaria:

Un tercio de las pérdidas es por falla eléctrica: subas y bajas de tensión, variación de frecuencia (f = f_i = factor de potencia) => variación del clock.

Potencia = VA = volt * amp

W = VA * f

Por ejemplo:

PC ≅ 1,5 A * 220 V * 0,8 (f_{PC} = 0,8 - 0,9) = 264 W

Monitor = 0,6 - 0,9 A

Impresora jet - ink = 0,4 A

Se deben sumar todos los consumos de los equipos (servers, hubs, routers, alarmas, equipos de control de acceso, etc.)

Potencia requerida = $\sum$ (A . factor de uso) + R

donde R suele estar entre el 20 y el 50% de A, pero el total no debe superar a A. Si el "factor de uso" no se conoce, se toma un equipo tipo con pinza amperométrica y se proyecta. El abastecimiento de baterías debe superar los 30 minutos para pequeños y medianos rangos y 60 minutos para mainframes.

III.7.2 Esquema básico de seguridad eléctrica en Centro de Cómputos:

III.7.2.1 Alimentación: dos líneas como mínimo, de distinta fuente (distintos proveedores o un proveedor y un generador propio). Las líneas deben ser puras, o sea no deben verse afectadas por corrientes reactivas provenientes de motores eléctricos u otras fuentes de interferencia.

III.7.2.2 <u>Tablero Principal:</u> debe contener en este orden:

- Llave seccionadora entre líneas de alimentación
- Llave de corte principal, asociado a botón golpe de puño
- Disyuntor diferencial sobre alimentación principal
- Llaves térmicas por cada línea de salida
- Salidas individuales para UPS, señal para iluminación de emergencia, aire acondicionado, equipos informáticos y equipos auxiliares (incluyendo iluminación normal)

El tablero debe estar cerrado con llave que debe estar en poder de personal de operación y Seguridad solamente.

III.7.2.3 <u>U.P.S.:</u> Recibe línea de alimentación única y entrega sólo a equipos informáticos y dispositivos de alarma y acceso físico.

III.7.2.4 <u>Alarmas y acceso:</u> los dispositivos de alarma y los de acceso al Centro de Cómputos, en caso de ser automatizado, debe ser permanente y su consumo y duración considerado en el cálculo de la UPS.

III.7.2.5 <u>Equipos Informáticos:</u> sólo los que intervienen en el procesamiento principal y sus comunicaciones, con alimentación de UPS y descarga a tierra independiente.

III.7.2.6 Aire acondicionado: el control de alimentación tanto de los compresores, calefactores y enfriadores de agua, deben estar en el Centro de Cómputos.

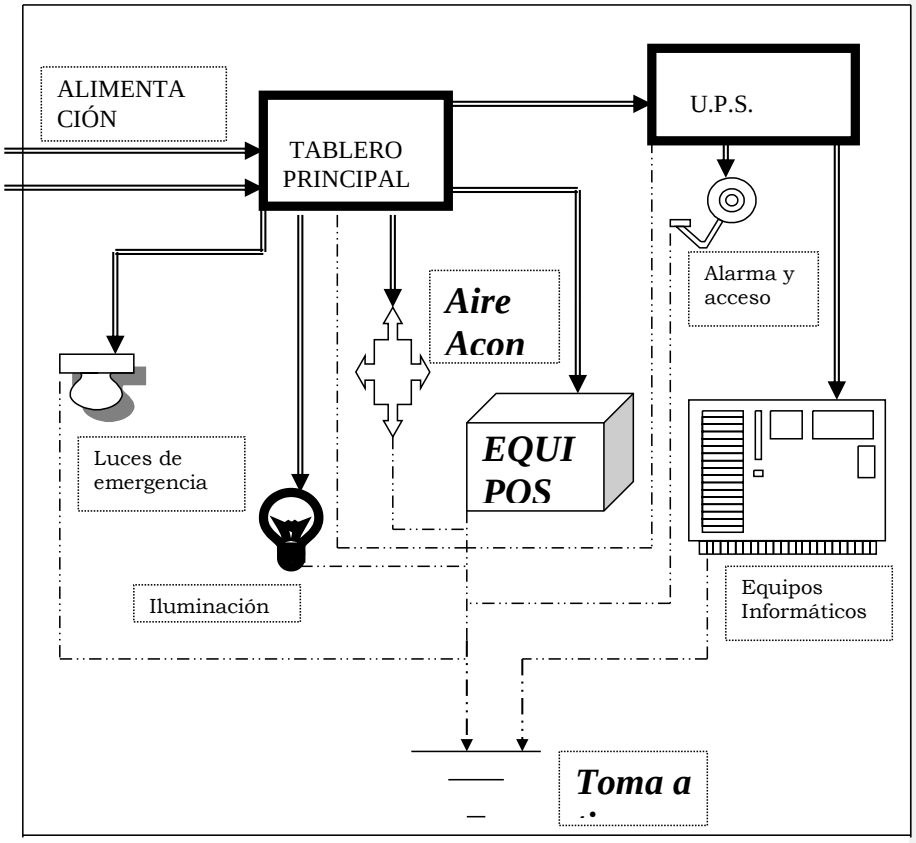
III.7.2.7 Equipos auxiliares: todos los que se encuentren en el Centro de Cómputos pero no intervienen en el procesamiento directamente, como fax, teléfonos, equipos de limpieza, destructoras de documentos, etc.

III.7.2.8 Iluminación: los equipos normales de iluminación deben controlarse desde el Centro de Cómputos, tanto los que están dentro de él como en sus accesos.

III.7.2.9 Iluminación de emergencia: reciba alimentación durante el abastecimiento normal de energía; al cortarse éste, automáticamente swichea a su alimentación independiente y se enciende. Su duración debe como mínimo duplicar la calculada para la UPS.

III.7.2.10 Toma a tierra: efectiva con resistencia menor a 1 Ω e independiente para los equipos informáticos del resto.

III.7.2.11 Esquema general:



III.8 <u>Seguridad en comunicaciones, tipos de enlaces y sus características principales:</u>

Los enlaces más comunes son:

- Telefónico: baja velocidad y confiabilidad, interfieren las ondas de radio, se usa para distribución urbana por MODEM, generalmente punto a punto. El costo es bajo y raramente se puede impedir incluirlas en alguna parte del enlace para poder llegar al usuario. Está siendo reemplazado casi en su totalidad para transmisiones de larga distancia.

- Microondas: alta velocidad pero con dificultad de instalación, ya que las antenas deben estar alineadas ya que las transmisiones se hacen solamente en línea recta de antena a antena. El costo es alto si se incluyen los equipos para repetir y aumentar las frecuencias que van en cada antena. Puede tener problemas por razones meteorológicas.

- Satelital: rápida y altamente confiable, sólo se interrumpe por grandes desastres naturales o mal uso de los canales.

- Fibra óptica: alta velocidad y totalmente confiable, sólo se interrumpe por rupturas.

Se suelen combinar por razones geográficas. Al determinar el tipo de enlace debe tenerse en cuenta que la velocidad de transmisión estará dada por la del enlace de velocidad mas baja, así como en la confiabilidad de los mismos.-

III : SEGURIDAD FÍSICA EN EQUIPOS Y DATOS

IV.1 Tolerancia a Fallos:

Es la posibilidad que un sistema siga funcionando sin interrupción, tras errores determinados fallos y afectando lo mínimo a su rendimiento (bancos, centrales telefónicas, sistemas de navegación, etc).
Se hace por redundancia, duplicación o RAID.

IV.1.1 Redundancia:

Es de las más usadas y consiste básicamente en la duplicación de determinados componentes del sistema, de forma que si uno de ellos cae, se conmute automáticamente a otro y el sistema continúe funcionando con normalidad. El componente del sistema se puede sustituir en caliente (funcionando).

IV.1.2 Duplicación:

Generalmente de discos rígidos, también se puede tener un duplicado de la computadora, se puede hacer con espejado (disk mirroring) para conmutación instantánea.

IV.1.3 Método RAID: (Redundant Array of Inexpensive Disk)

Es una técnica en la que un o más disk - pack se usan como si fuera un disco sólo, lo que da mayor seguridad además de mejorar la performance del sistema.

Básicamente se dividen los datos en formatos que puede ser sectores, bytes o bits y se distribuyen en las distintas unidades, registrando además la información de paridad.

Si una de las unidades falla y se produce una pérdida de información, se podrá reconstruir por completo con la información de paridad y la del resto de las unidades.

Al poder leer y escribir simultáneamente sobre todas las unidades se produce un aumento de rendimiento, dado que el archivo se repetirá por las distintas unidades y actuará con las cabezas lectoras - grabadoras al mismo tiempo.

Se necesita una unidad extra cada dos o más unidades primarias con un grado de seguridad alto y generalmente eficiente, lo que sensiblemente más económico que la duplicación o mirroring tradicional; la probabilidad de pérdida está dada cuando fallan dos

unidades simultáneamente y pierdan la información del mismo fragmento, la cual es muy baja.

Hay varios niveles de RAID según la protección, yendo los mas comunes desde 0, donde sólo se fragmenta la información y se reparte en las unidades a grabar datos de paridad, hasta 5 donde se registra toda la información de paridad repartida entre todas las unidades (≅ ¾ para datos y ¼ para paridad). Novell y NT soportan RAID. Ya existen otros niveles para aplicaciones especiales.

IV.1.3.1 Funcionamiento del RAID:

El posicionamiento de la cabeza del disco está limitado por dos factores: el ***tiempo de búsqueda*** (seek time) y el ***retardo por el giro del disco*** hasta la posición de inicio de los datos (latencia rotacional). La transferencia de datos, por su parte, ocurre de a un bit por vez y se ve limitada por la velocidad de rotación y por la densidad de grabación del medio.

Una forma de mejorar el rendimiento de la transferencia es el ***uso de varios discos en paralelo;*** esto se basa en el hecho de que si un disco solitario es capaz de entregar una tasa de transferencia dada, entonces dos discos serían capaces, teóricamente, de ofrecer el doble de la tasa anterior. La adición de varios discos, formando uno o más cilindros, debería extender el fenómeno hasta un punto a partir del cual algún otro componente del sistema de lectura / grabación, buffer o disco, empezará a ser este componente el factor limitante.

Las soluciones de estos arreglos basadas en hardware son principalmente implementadas mediante el uso de controladoras **SCSI** (Small Computer System Interface) especializadas, las cuales a menudo están dotadas de procesadores propios para liberar a la CPU del sistema de la tarea de control y de cachés para mejorar aún más el desempeño.

En la práctica, sin embargo, los niveles teóricos de mejoramiento **no** se obtienen debido, principalmente, a la carga de trabajo inherente al control del propio arreglo. Además el uso de varios discos se emplea para construir cierto nivel de redundancia de los datos y es este nivel de redundancia y la forma de implementarlo lo que crea los niveles de RAID.

IV.1.3.2 RAID Hardware

Las soluciones hardware gestionan el subsistema RAID independientemente del host, presentándole a este un solo disco.

Un ejemplo de RAID hardware podría ser el conectado al controlador SCSI que presenta al sistema un único disco SCSI. Un sistema RAID externo se encarga de la gestión del RAID con el controlador localizado en el subsistema externo de los discos. Todo el subsistema está conectado a un host a través de un controlador SCSI normal y se le presenta al host como un solo disco.

IV.1.3.3 RAID Software

El RAID Software implementa los diferentes niveles de RAID en el código del kernel que tienen que ver con la gestión del disco (block device). Ofrece además la solución menos costosa, el RAID software funciona con discos IDE menos costosos así como con discos SCSI. Con las rápidas CPU de hoy en día, las prestaciones de un RAID software pueden competir con las de un RAID hardware.

Striping es el acto de unir dos o más discos físicos en un solo disco lógico con el fin de dividir los datos entre los diferente discos para ofrecer una significativa mejora en el rendimiento del conjunto de los discos.

IV.1.3.4 Tipos de arreglos:

- Arreglos paralelos: éstos son aquellos en que cada disco participa en todas las operaciones de entrada / salida. Este tipo de arreglo ofrece ***tasas altísimas de transferencia*** debido a que las operaciones son distribuidas a través de todos los discos del arreglo y ocurren en forma prácticamente simultánea. La tasa de transferencia será muy cercana, 95%, a la ***suma de las tasas de los discos miembros***, mientras que los índices de operaciones de entrada / salida serán similares a las alcanzadas por un disco individual. En síntesis, ***un arreglo paralelo accesará sólo un archivo a la vez pero lo hará a muy alta velocidad***. Algunas implementaciones requieren de actividades adicionales como la sincronización de discos.

Los RAID de niveles 2 y 3 se implementan con arreglos paralelos.

- Arreglos independientes: son denominados así aquellos arreglos en los cuales cada disco integrante opera en forma independiente, aún en el caso de que le sea solicitado atender varios requerimientos en forma concurrente. Este modelo ofrece ***operaciones de entrada / salida sumamente rápidas*** debido a que cada disco está en posición de atender un requerimiento por separado ya que cada archivo está alojado en un solo disco.

  Los niveles 4 y 5 de RAID se implementan con arreglos independientes, mientras que los niveles 0 y 1 pueden ser implementados tanto en forma de arreglos independientes como en arreglos paralelos.

IV.1.3.5 Tipos de RAID:

- Lineal : Diferentes discos se enlazan uno detrás de otro para que el sistema vea un solo disco más grande. Si falla uno se pierde todo el sistema de ficheros.

- RAID 0 : La información se graba y se lee en paralelo entre varios discos. Como no hay redundancia el riesgo de fallos es el mismo, pero el rendimiento es muy bueno.

- RAID 1 : Mirrored Disk Array (MDA), conjunto de discos en espejo: esta configuración incluye dos unidades de disco: una unidad de datos y una unidad de réplica. Cuando se escriben datos en una unidad, también se escriben en la otra. El disco redundante es una replica exacta del disco de datos, por lo que se conoce también como disco espejo. Los datos pueden leerse de cualquiera de las 2 unidades de forma que si se avería la unidad de datos es posible acceder a la unidad de réplica, con lo que el sistema puede seguir funcionando. Con el nivel de RAID se obtiene la misma velocidad de lectura / escritura que una configuración normalizada de disco, por lo que constituye la mejor opción para aplicaciones que contienen un gran número de operaciones de escritura.

Como ventajas tiene mayor rendimiento en las lecturas de datos que las lecturas convencionales y permite recuperar todos los datos en caso de error en unos de los discos, ya que si un disco suspende la operación el otro continua disponible.

Su principal desventaja es el alto costo, ya que se usa el doble de espacio que el necesario.

RAID 1 esta diseñado para sistemas en donde la disponibilidad de información es esencial y su reemplazo resultaría difícil y costoso (mas costoso que reponer el disco en si). Típico en escrituras aleatorias pequeñas con tolerancia a fallas. El problema de este tipo de arreglos es el costo que implica duplicar el disco.

- RAID 2 : Hamming Code for Error Correction :

  Es el primer nivel de RAID que usa código de correcciones de error utilizando de código de error Hamming.

  Este nivel cuenta con varios discos para bloques de redundancia y corrección de errores. La división es a nivel de bits, cada byte se graba con un bit de paridad en cada uno de los discos y un bit de paridad en el noveno. El acceso es simultaneo a todas las unidades tanto en operaciones de escritura como lectura. Algunos de estos discos son empleados para códigos de error, los cuales se emplean para referencias de los datos en caso de que falle uno de los discos.

  Este nivel tiene un costo bastante elevado ya que son necesarios muchos discos para mantener los códigos de error. Gracias a como están distribuidos los datos en los discos se consigue mejorar la velocidad de transferencia principalmente en la lectura ya que permite emplear todos los discos en paralelo. Estos discos aunque proporcionen un buen rendimiento no son muy empleados ya que los niveles 1 –3 – 5 proporcionan una mayor relación costo / rendimiento.

  Su ventaja principal es que puede recuperar todos los datos gracias a los discos de código de error.

  Su costo es alto ya que requiere muchos discos para guardar los códigos de error y tiene tiempos de escritura de datos bastante lentos, incluso aunque los datos se separen en diferentes discos

- RAID 3: Sistemas de discos en paralelo con disco de paridad para corrección de errores, conocido también como Striping. Utiliza un disco de protección de información separado para almacenar información de control codificada con lo que se logra una forma mas eficaz de proporcionar redundancia de datos. Este control de información codificada o paridad proviene de los datos almacenados en los discos y permite la reconstrucción de información en caso de fallas. Se requieren como mínimo 3 discos y se utiliza la capacidad de un disco para manejar rápidamente la información de control. Los datos se dividen en fragmentos que se transfieren a los discos que funcionan en paralelo, lo que permiten enviar mas datos de una sola vez, y aumentar en forma sustancial la velocidad general de transferencia de datos. Esta ultima característica convierte a este nivel en idóneo para que estas aplicaciones que requieran la transferencia de grandes ficheros contiguos hacia y desde el ordenador central.

  Resultan mas adecuados para sistemas en los que transfieren grandes cantidades de datos secuencialmente, por ejemplo audio, video, archivos maestros, etc. Es menos apropiado para el tipo de acceso de base de datos en los cuales se necesitan transferir pequeñas unidades de datos de manera aleatoria.

  En aquellos entornos en los que muchos usuarios desean leer y escribir múltiples registros aleatorios, las peticiones de operaciones de entrada /salida simultaneas pueden sobrecargar y ralentizar el sistema. En el nivel 3 de RAID todos los discos participan en cada transacción, atendiendo cada petición de Entrada /Salida de una en una. Por consiguiente el nivel 3 de RAID no es una opción adecuada para operaciones transaccionales, en la que la mayor parte del tiempo se emplea en buscar pequeños registros esparcidos aleatoriamente en los discos.

  Su principal ventaja es entonces el alto rendimiento para aplicaciones de velocidad de transferencia alta y gran volumen de datos secuenciales, con la posibilidad, gracias al disco de paridad, de poder recuperar todos los datos.

  Sin embargo, debe tenerse en cuenta que si se pierde el disco de paridad también se pierde toda la información redundante, aunque es altamente improbable.

- RAID 4, Independient Disk Array (IDA):

  Sistemas de discos independientes con disco de control de errores. En este nivel los bloques de datos pueden ser distribuidos a través de un grupo de discos para reducir el tiempo de transferencia y explotar toda la capacidad de transferencia de datos de la matriz de disco. El nivel 4 de RAID es preferible al nivel 2 de RAID para pequeños bloques de datos , por que en este nivel los datos son distribuidos por sectores y no por bits. Otra ventaja del nivel 4 de RAID frente a los niveles 2 y 3 es que al mismo tiempo puede estar activa mas de una operación de lectura / escritura sobre el conjunto de discos .

  Cada disco graba un bloque de datos distinto, y un disco adicional graba un código de corrección de errores. Si falla un disco, su información se puede recomponer; solo se pierde la capacidad de un disco.

  El nivel 4 de RAID tiene división a nivel de bloques y el acceso al arreglo de discos es paralelo, pero no simultaneo. Posee un sistema de paridad y corrección de errores. La operación de escritura se realiza en forma secuencial y la lectura en paralelo.

  Tiene buen rendimiento en las escrituras de datos, asegurando la integridad de los mismos.

  Como inconvenientes debe tenerse en cuenta que si se pierde el disco de paridad, se pierde toda la información redundante; también tiene menor rendimiento en las lecturas de datos

- RAID 5:

  Igual que el anterior, pero el disco que graba el código de corrección se va alternando. Rápido, seguro, y sólo pierde la capacidad de un disco, pero necesita al menos 3 discos.

- RAID 6:

  Este tipo es similar al RAID-5, pero incluye un segundo esquema de paridad distribuido por los distintos discos y por tanto ofrece tolerancia extremadamente alta a los fallos y las caídas de disco.

- RAID 7:

  Este tipo incluye un sistema operativo incrustado de tiempo real como controlador, haciendo las operaciones de caché a través de un bus de alta velocidad y otras características de un ordenador sencillo.

- RAID 10:

  La información se distribuyen en bloques como el RAID 0 y adicionalmente, cada disco se duplica como RAID 1 , creando un segundo nivel de arreglo se conoce como "Striping de arreglos duplicados". Se requieren dos canales, dos discos para cada canal y se utilizan el 50 % de la capacidad para información de control.

  Este nivel es de altísima seguridad dado que ofrece un 100 % de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante. Es ideal para sistemas de emisión critica, donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escritura aleatorias pequeñas.

- RAID 30:

  Es ideal para aplicaciones no interactivas, tales como señales de grafico e imágenes. Se conoce también como “Striping de arreglos de paridad dedicada”. La información es distribuida a través de los discos, como en RAID 0 y utiliza paridad dedicada, como RAID 3, en un segundo canal; requiere mínimo 6 discos. Proporciona una alta confiabilidad igual que el RAID 10 ya que también es capaz de tolerar dos fallas físicas en canales diferentes , manteniendo la información disponible.

- RAID 50:

  Esta diseñado para aplicaciones que requieren un almacenamiento altamente confiable una elevada tasa de lectura y un buen rendimiento en la transferencia de datos;

con un nivel de RAID 50, la información se reparte en los discos y se usa paridad distribuida, por eso se conoce como "Striping de arreglo de paridad distribuidas". Se requiere mínimo 6 discos. Se logra confiabilidad de la información, un buen rendimiento en general y además soporta grandes volúmenes de datos. Igualmente si dos discos sufren fallas físicas en diferentes canales, la información no se pierde.

RAID 50 es ideal para aplicaciones que requieran un almacenamiento altamente confiable, una elevada tasa de lectura y un buen rendimiento en la transferencia de datos .A este nivel se encuentran aplicaciones de oficina con muchos usuarios accediendo a pequeños archivos, al igual que procesamiento de transacciones.

- RAID 53:

Este tipo ofrece un conjunto de bandas en el cual cada banda es un conjunto de discos RAID 3. Esto proporciona mejor rendimiento que el RAID 3, pero a un costo mucho mayor.

IV.1.3.6 Ventajas generales del RAID:

Los discos optimizados para RAID poseen circuitos integrados que detectan si el disco está fallando, de ser así este circuito se encargará por encima del tiempo real de sacar la información y almacenarla en los otros discos, o si es el caso en el "hot spare". Un hot spare es un disco que permanece siempre en el sistema esperando a que otro se estropee y él entre directamente en funcionamiento.

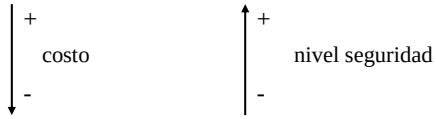
Una de las ventajas del sistema RAID es la posibilidad, con los discos hot swap, de conectarlos y desconectarlos en "caliente", es decir, que si un disco falla no hará falta el apagar el sistema para remplazarlo.

Permite reconstrucción y regeneración, cuando un disco falla la información redundante en los discos y los datos en los discos buenos son usados para regenerar la información de disco averiado.

IV.2 Mantenimiento de los equipos:

Existen tres tipos de mantenimiento:

- Preventivo
- Predictivo
- A demanda



- Preventivo: consiste en reemplazar las piezas basados en un parámetro de uso (tiempo, cantidad de hojas impresas, cantidad de unidades grabadas) sin considerar el estado de las mismas. Son pocas las piezas que son mantenidas con ésta técnica.

- Predictivo: consiste en revisar las piezas en ciclos determinados y, mediante un diagnóstico, decidir su reemplazo o no. En general se aplica con la limpieza del equipo.

- A demanda: cuando se produce una rotura.

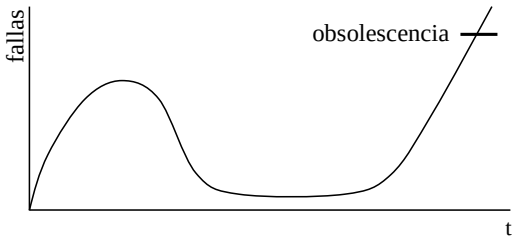
IV.2.1 Contratos de Mantenimiento:

- Por abono: el mantenedor reparará el equipo en un tiempo especificado facturando sólo el costo de las piezas dañadas por mal uso.

- Por llamado: garantiza la concurrencia de un técnico en un plazo determinado.

IV.2.2 Registro de fallas:

Para estadísticas de fallas y punto de obsolescencia también para el control del mantenedor.



IV.3 Aspectos a tener en cuenta en la Seguridad del Mantenimiento:

IV.3.1 Para contratar:

- Representante local.
- Stock de repuestos, tiempo de disponibilidad.
- Posibilidad de equipos de reemplazo.
- Calidad de los mantenedores.
- Antecedentes de otros contratos.

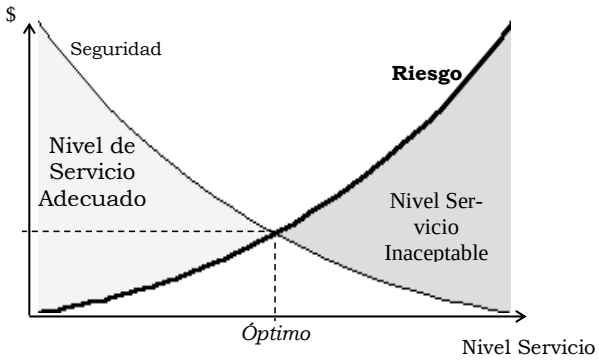
IV.3.2 Para el acceso y el traslado:

- Control de personal ingresado y egresado.
- Presencia siempre de un operador para observar y para seguridad del mantenedor.

IV.3.3 Para automantener:

- Guía de servicio.
- Repuestos y filtros.
- Limpieza, personal de mantenimiento.
- Pruebas de líneas eléctricas y de comunicaciones alternativas.

IV.3.4 Evaluación de seguridad vs. nivel de servicio:



IV.4 Medidas comunes de seguridad en Operación:

Ver el punto ***Controles*** en el ***Anexo 1.***

- Bitácora: es una planilla en el que el operador registra:

- Fecha
- Hora
- Nombre de operador
- Novedad
- Solución
- A quién se comunicó

- Hoja de Ruta: flow de operación integral.

- Esquenas de Distribución: de salidas, listado, archivos y soportes. Horarios y responsables.

- Programa Operativo según Ciclos: según los ciclos que se cumplen en el día.

IV.5 Resguardo de Datos:

- Back - Up: copia ***recuperable*** duplicada del original. Puede ir desde datos individuales, archivos, bibliotecas o los soportes íntegros.
- Cantidad: cantidad necesaria + 1.
- Importancia: sólo igualable a la eficiencia del proceso en sí.

IV.5.1 Tipos de Back - Up:

- Completo o 100%: Se debe hacer por lo menos una vez para luego continuar con otros; es la mejor pero es cara ya que para que sea efectiva debe incluir programas, archivos, comandos, etc.

- Progresivo: se copian sólo los archivos creados o modificados desde el último Back Up, completo o progresivo. La copia total será la formada por la última completa y el procesamiento cronológico de las progresiones en el orden que se efectuaron. Puede ser para todo el sistema o para un archivo en particular. Debe guardarse un número importante de copias, mínimo un ciclo.

- Diferencial: copia sólo los ficheros modificados o creados desde la copia completa, o sea que contiene las diferencias entre el estado original y el último. Al restaurar se levanta la copia total y la diferencial, resultando más simple y económico, pero sin permitir restauraciones a estados intermedios.

IV.5.2 Planificación del Back – Up:

Se planifica en función de los siguientes aspectos:

- volumen de datos de cada sistema
- ciclo de trabajo
- frecuencia dentro del ciclo
- qué datos se copian
- en qué momento se copian
- tiempo de demora de la copia
- qué soporte se empleará
- que tipo de back - up se hará (progresivo, diferencial, etc.)
- lugar de almacenamiento
- período de retención
- riesgos (nivel de servicio y costos)
- sistema de registración y control

IV.5.3 Elección del Tipo de Copia:

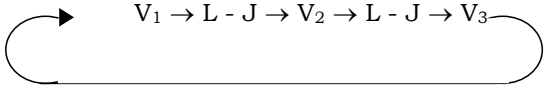
Según el tipo de aplicación y la velocidad de restauración.
El diferencial suele ser el más adecuado pero combinado con un esquema Abuelo, Padre, Hijo o Lu - Vi. Hay que tener en cuenta que el ciclo de control suele ser menor al de utilización.

- Ciclo de copias: Se hace en periodos de cierta duración y se reusan los soportes. Al cierre de los ciclos de utilización (año fiscal, por ejemplo) se hacen copias completas.

  La rotación de soportes (A,P,M o Lu- Vi) puede tener variantes:

  - V completa - L a J programada y repetir.
  - L - V doble, igual al anterior pero el segundo V se comienza con un segundo juego y el L a J siguiente se hacen progresivas

desde éste último. En el tercer V se tomará de nuevo el primer juego y así sucesivamente:



- A, P, H extendido: se etiquetan 7 copias: Diaria, V1, V2, V3, M1, M2 y M3. Se comienza un Viernes a última hora con copia completa en V1. De L a J se hacen progresivas sobre Diaria; el Viernes completa sobre V2. La semana que sigue sobre Diaria y el Viernes sobre V3. Luego progresiva igual de L a J y el Viernes sobre M1, y se repite hasta 3 meses:

DÍA	TIPO	1° MES	2° MES	3° MES
V	Completa	V1	V1	V1
L - J	Progresiva	D	D	D
V	Completa	V2	V2	V2
L - J	Progresiva	D	D	D
V	Completa	V3	V3	V3
L - J	Progresiva	D	D	D
V	Completa	M1	M2	M3
L - J	Progresiva	D	D	D

IV.6 Control de Input:

Ver el punto ***Controles*** en el ***Anexo 1.***

IV.7.1 Totales: el control de totales de los datos a ingresar es una forma rápida de detectar fallas; estos pueden ser generales, de lote o por muestreo.

- Muestreo: se trata de decidir a quién o que se observará; se utiliza cuando el tamaño de la población a relevar es de una magnitud que hace imposible su análisis total.

  Muestreo de datos es el proceso sistemático por el cual se seleccionan elementos representativos de una población. Al ser investigados, su análisis se hará extensivo a toda la población con un cierto grado de certeza.

  Con el muestreo se logra bajar costos de control de datos, mejorar la eficacia, agilizar el procesamiento y minimizar la parcialidad. Los pasos a seguir son:

  1. determinar los datos que se van a recopilar

2. determinar la población
3. elegir el tipo de muestra
4. decidir el tamaño de la muestra

Los puntos 1 y 2 tienen que surgir de informaciones previas. Para el paso 3, **tipos de muestras,** se debe elegir según el grado de compromiso del dato entre:

- determinísticas: se determinan en base a un criterio lógico, no probabilístico:
    - de oportunidad: son las más simples; el criterio se toma al azar; por ejemplo, cuantos lotes de cheques hay para controlar en un salón entre las 20 y las 22 horas un día de semana.
    - dirigidas: el analista elige las personas o datos a muestrear en base a un criterio; por ejemplo, cuantos lotes de cheques hay que controlar a distintas horas, distintos días y en distintas épocas. Es medianamente confiable.
- probabilísiticas: se basan en algún criterio estadístico:
    - aleatorias simples: se numera la población y se asegura que cada miembro de ella tenga la misma oportunidad de ser elegido. Por ejemplo, ordenar un archivo y seleccionar por generación de numeros al azar.
    - aleatorias complejas: es el mejor para las tareas de análisis. Sus enfoques son:
        - muestreo probabilísitico: por ejemplo tomar el enésimo número de una lista y repetir a períodos iguales. Es simple y eficaz pero se debe asegurar que el ordenamiento de la lista no representa periodicidad de ningún tipo. No es útil para documentos.
        - muestreo estratificado: se identifican subpoblaciones (estratos) y dentro de ellos a los sujetos probabilísticamente.
        - muestreo por grupos: se selecciona un grupo por considerarlo prototípico.

El paso 4, ***tamaño de la muestra***, se maneja según dos criterios: por atributos y por variables. El analista determina la precisión deseada (intervalo aceptable) y el error standard (nivel de confianza). Estas

limitaciones más las características de la población son las que determinan el tamaño de la muestra.

- Determinación por atributos: da la proporción precisa de un tipo de información y el porcentaje que presenta errores. Los pasos son:
    1. establecer el atributo que se va a muestrear
    2. localizar donde están esos atributos
    3. examinar el atributo y estimar **p** (proporción de la población que cuenta con ese atributo)
    4. determinar **i** (intervalo aceptable)
    5. decidir el nivel de confianza y sacar el coeficiente ***z*** de tablas; un ejemplo de tablas de coeficiente de confiabilidad:

Nivel de confianza %	**Coeficiente de confiabilidad *z***
99	2,58
98	2,33
97	2,17
96	2,05
95	1,96
90	1,65
80	1,28
50	0,67

    6. calcular el error standard ***Vp = i/z***
    7. deteminar el tamaño de la muestra **n** aplicando:

$$n = \frac{p \cdot (1 - p)}{Vp^2} + 1$$

Como valores habituales **p** se toma entre 0,10 y 0,50; **i** suele ser ± 0,10 y el nivel de confianza del 95%. Evidentemente el tamaño de muestra aumenta cuando es mayor el nivel de confianza o un intervalo de confianza más pequeño. Cuando no se poseen suficientes antecedentes, se debe elegir una muestra pequeña, se aplican los valores elegidos y, analizando el resultado, iterar los pasos con los valores convenientes.

- Determinación por variables: proporciona información de carácter cuantitativo, por ejemplo cantidad de devoluciones de mercadería, ventas totales, número de errores procesado, etc. Los pasos son similares, pero se basan en la variación de la desviación standard **s**:
    1. determinar la variable a muestrear
    2. localizar la base de datos donde se podrán recuperar los valores de las variables

3. examinar la variable para determinar dispersión y magnitud; idealmente, convendría conocer el valor promedio y la desviación standard **s**
4. subjetivamente se determina **i,** el intervalo aceptable
5. se elige un nivel de confianza y se busca en tablas el coeficiente de confiabilidad ***z***
6. se calcula el error standard del promedio de los valores de las variables como ***Vx = i/z***
7. se determina el tamaño de la muestra **n:**

$$n = \left(\frac{s}{Vx}\right)^2 + 1$$

Se puede iterar a partir del paso 3; el intervalo está en función directa de la cantidad analizada, por ejemplo, para una información diaria de 100.000 registros un intervalo de 100 (0,001) es bajo; para una información de 5.000$ (0,02) es aceptable.

IV.7.2 <u>Verificar:</u>

- ✓ Porcentaje de datos que se reciben.
- ✓ Cabeza de lote:
  - Fecha y hora de envío
  - Área que lo envía
  - Formato
  - Usuario que lo envía
  - Quién lo recepciona
  - Cantidad de registros para grabar
  - Totales de uno o más campos
  - Fecha y hora de recepción
  - Quién lo graba
  - Observaciones
- ✓ Dígito verificador: el algoritmo debe aplicarse en todas las cifras posibles a ingresar. Tratar de usar aquellos que tienen menor posibilidad de gemelos, por ejemplo el Módulo 11 Geométrico:

  2 9 6 4 5

  x32 x16 x8 x4 x2

  ---- ---- ---- ----- ----

  64 + 144 + 48 + 16 + 10 = 282 / 11 = 25 resto 7

  DV = 11 – 7 = 4; el dato debe venir informado como 29645/4.

- ✓ Controles:
  - Firmas que correspondan
  - Calidad de la fuente (legibilidad, integralidad, exactitud de totales)
  - Prioridades de captación
  - Costos de control
  - Razonabilidad en el tamaño de los lotes
- ✓ Programa de carga:
  - Frecuencia con que se hace
  - Fijación de prioridades
  - Hachones que se toman si no se reciben en los tiempor programados
- ✓ Procedimiento:
  - Qué se hace con los totales y documentos inválidos
  - Registros de anomalías
  - Proceso de almacenamiento de documentos
  - Control de producción por persona
- ✓ Control por código de barras.

IV.8 <u>ATM:</u> (Automathic Threller Machine)

Conjunto de equipos que manejan volúmenes de transacciones grandes.

- <u>Tipos:</u>

- cajero automático
- buzones de pago
- guías
- de reservas (tarjeta de crédito)

- <u>Tarjetas magnéticas que usan los ATM:</u>

- de crédito: ingreso a cajeros para hacer consultas de saldo y retirar montos de dinero
- de débito: manejar caja de ahorro, con un banco determinado

- <u>Aplicaciones extras de los ATM:</u>

- toma de créditos

- emisión de pólizas de seguros

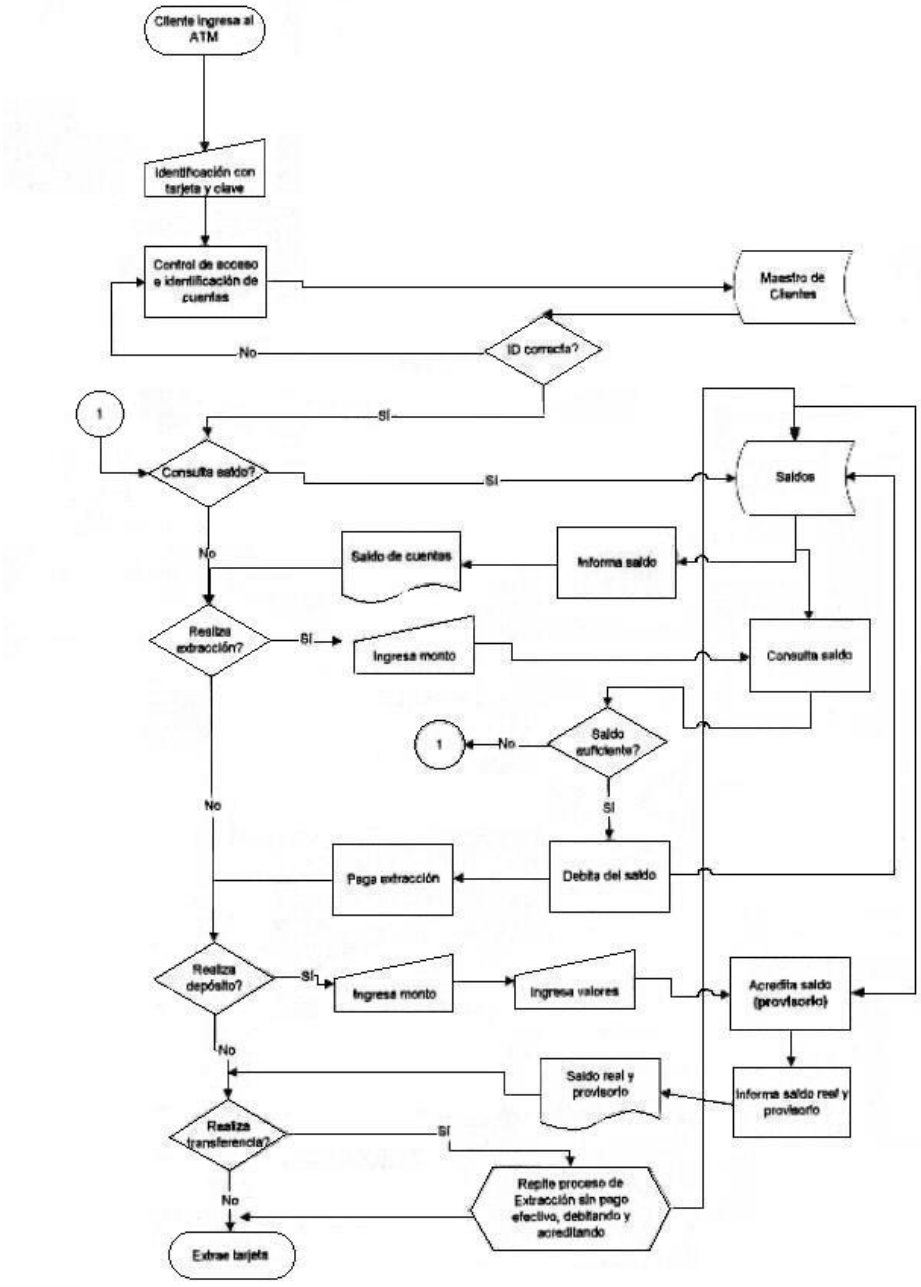
- pago de facturas de servicios por débito

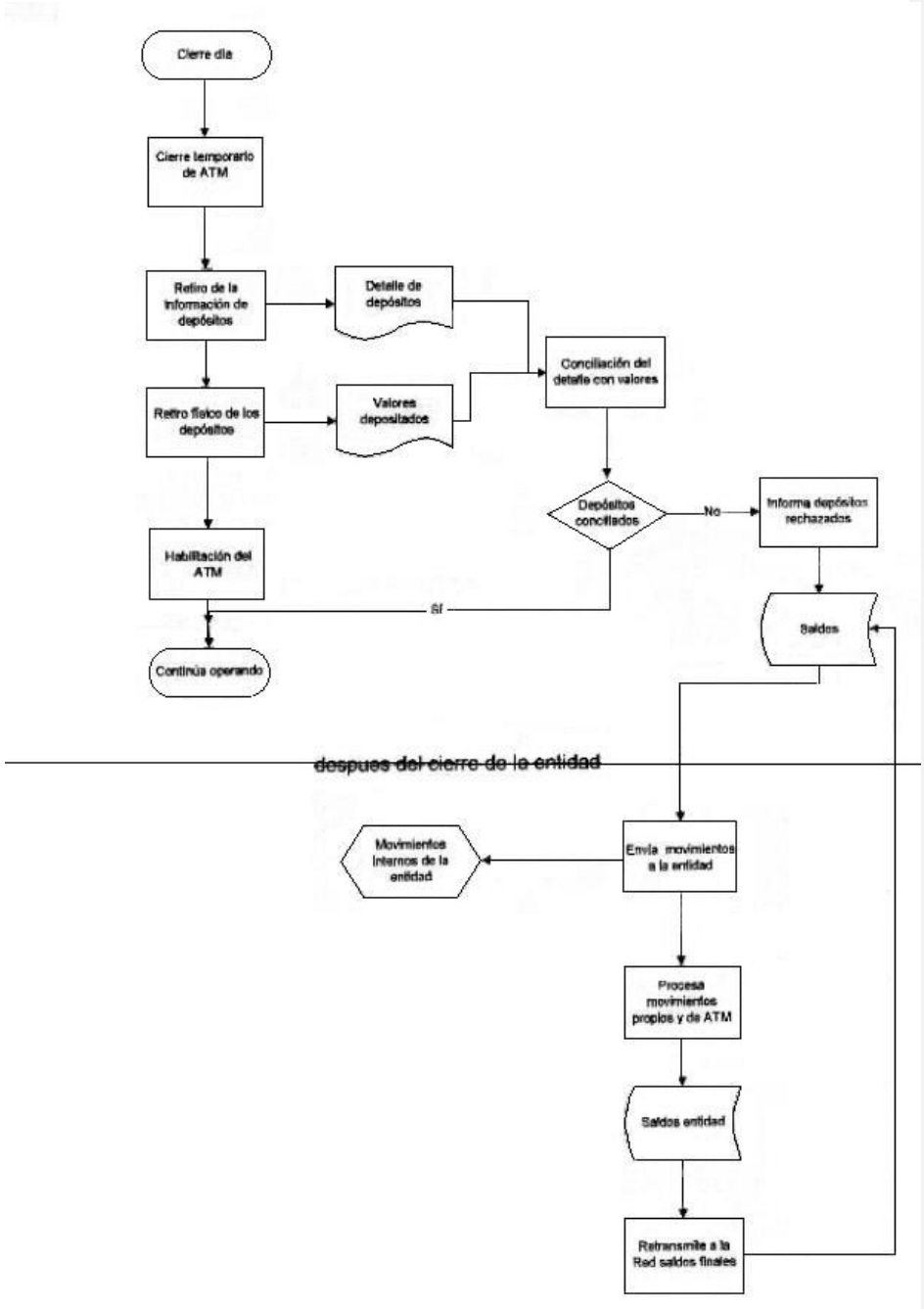
- pago de cuotas de comercios

- donaciones

Existen problemas de seguridad en los momentos de cierre de los ATM para que realicen sus procesos batch y en la intercomunicación con las entidades financieras para mantener en todo momento los mismos saldos en las cuentas.

Son similares los problemas que se presentan en el home – banking y en los pagos con tarjetas o por débito de cuentas mediante Internet, aunque aquí se deben agregar los riesgos por intromisiones dada la baja seguridad de la red.-


Cliente ingresa al ATM
Identificación con tarjeta y clave
Control de acceso e identificación de cuentas
Maestro de Clientes
ID correcta?
No
Si
1
Consulta saldo?
Si
Saldos
No
Saldo de cuentas
Informa saldo
Realiza extracción?
Si
Ingresa monto
Consulta saldo
1
No
Saldo suficiente?
Si
No
Paga extracción
Debita del saldo
Realiza depósito?
Si
Ingresa monto
Ingresa valores
Acredita saldo (provisorio)
No
Saldo real y provisorio
Informa saldo real y provisorio
Realiza transferencia?
Si
No
Repite proceso de Extracción sin pago efectivo, debitando y acreditando
Extrae tarjeta


Cierre día
Cierre temporario de ATM
Retiro de la información de depósitos
Detalle de depósitos
Retiro físico de los depósitos
Valores depositados
Conciliación del detalle con valores
Depósitos conciliados
No
Informa depósitos rechazados
Habilitación del ATM
Si
Saldos
Continúa operando
después del cierre de la entidad
Movimientos internos de la entidad
Envía movimientos a la entidad
Procesa movimientos propios y de ATM
Saldos entidad
Retransmite a la Red saldos finales

V: INTRODUCCIÓN A LA SEGURIDAD LÓGICA

La base de la Seguridad Lógica, o sea de la información archivada o transmitida, es sin duda la Criptografía, pero existen algunas consideraciones especiales. La importancia de los ataques directamente sobre los datos se ha incrementado notablemente en los últimos tiempos por efecto del uso de Internet, el uso intensivo de bases de datos, la popularización y facilidad de uso de los sistemas operativos y los recursos disponibles para el ataque que son cada vez mayores y mas conocidos.

En una encuesta reciente en EEUU, sobre más de 500 empresas de distinto tamaño y distintas ramas de la industria y los servicios, se detectaron los siguientes datos (94% de ellas tienen site en la Web):

- 61% de pérdidas por uso no autorizado del sistema
- 32% están usando métodos seguros de identificación para operar en Internet
- Promedio de pérdida por robo de información de 1.200.000 u$s
- Promedio de pérdida por sabotaje de datos de 1.100.000 u$s
- 50 % de abuso del uso de la red

En cuanto al tipo de seguridad lógica que usa en sus archivos:

- 89% control de acceso lógico
- 88% Firewalls
- 59% criptografía
- 59% sistemas de passwords tradicionales
- 44% Passwords cifradas (para log – in)

Con respecto a las fuentes de ataque más frecuentes:

- 86% empleado disconforme
- 74% hacker independiente
- 53% competidores comerciales

La Seguridad Lógica debe garantizar que las transmisiones de datos y, óptimamente, los datos que se extraen de los archivos tengan:

- Integridad: la información sea la solicitada, sólo esa sin extracciones, agregados o modificaciones.

- Autenticidad: comprobar que el emisor y el receptor de la información sean quienes dicen ser y estén autorizados para desempeñarse como tales.

- No rechazo: anular la posibilidad de negación de recepción de una información, por medio de registros inaccesibles fuera de los procesos autorizados.

V.1 Seguridad en Bases de Datos:

Las Bases de Datos, a diferencia de los archivos planos, tienen características especiales de estructura para su propio funcionamiento que las hacen mas sensibles a posibles ataques. Su propio esquema puede servir de guía al intruso para aprovechar las porciones de información que posee y así lograr sustraer o estropear información.

V.1.1. Tipos de ataques:

- Ataque a la información sensible: cuando es descubierta por un individuo desautorizado.
- Alteración no autorizada.
- Ataques que causan que la información sea inaccesible a los individuos autorizados.

Los asaltadores de la base de datos generalmente tienen la opción de atacar a las aplicaciones directamente, o de atacar al sistema operativo subyacente. El último es un problema más difícil ya que si no se conocen las vulnerabilidades del sistema operativo es casi imposible realizarlo.

Los ataques se basan en los problemas de:

- Inferencia: Este problema involucra a un asaltador malévolo que combina la información disponible en la base de datos con el análisis conveniente para inferir información que está presumiblemente oculta.

- Agregación: Este problema se da cuando los pedazos de información que no son sensibles por separado se convierten en sensibles cuando se los reúnen.

  La base de datos que tenga este problema podría tratarse permitiendo etiquetar los pedazos como no sensibles, pero

cuando una colección o agregado se crea, por alguna pregunta del usuario, la base de datos podría actualizarse de modo que este agregado sea sensible.

Un acercamiento alternado que podría tomarse para tratar con este problema de agregación involucra el etiquetado de los pedazos como sensibles. Los agregados se etiquetarían como sensibles a menos que ellos representen adecuadamente el subconjunto de no sensibles de información, en ese caso el agregado se etiquetaría como no sensible.

- Multiinstanciación: La técnica conocida como instanciación involucra varias vistas de un objeto para determinados usuarios. El contenido de la vista dependerá de los atributos de seguridad para ese usuario.

V.1.2 Firewalls

- Definición de una Firewall de RED:

Un Firewall es un sistema que permite establecer una política de control de acceso entre dos redes. Básicamente tiene dos mecanismos: uno para bloquear tráfico y otro para permitir tráfico.

Las Firewalls actúan igualmente como detectores de intrusiones, no solo bloqueando el acceso sino identificando al intrus, ya sea por su dirección, actuación en el tráfico, etc., dejando registros para posteriores auditorías.

Las Firewalls protegen contra todo lo que las pretenda atravesar, pero sobre todo en bases de datos es común encontrar "puertas traseras" que facilitan accesos no autorizados. Lo mismo sucede con Internet cuando no se conocen con exactitud los protocolos de ingreso.

Tampoco protege contra sustracciones de las personas autorizadas al acceso, por rezones dolosas o simple curiosidad. El pasaje de información a soportes extraíbles es un riesgo mayor a cualquier intrusión en las bases de datos. Tampoco lo hace contra virus, a menos que estos realicen una intrusion no autorizada.

La definición de las políticas a usar en las Firewalls depende, en primer lugar, del nivel de monitoreo, redundancia y control que la Gerencia quiere, definido como el nivel de riesgo aceptable. El alto

costo de las Firewalls y de su instalación y personalización es otro factor a tener en cuenta.

- Tipos de Firewalls:

  - Nivel de Red: este nivel generalmente toma sus decisions basadas en las direcciones y puertos de origen y destino de los paquetes individuales de IP. El nivel tradicional de Firewall de Red es el Router, aunque no permite tomar decisiones sofisticadas.

  - Nivel de Aplicación: tienen alto refinamiento de parametrización. Generalmente son host corriendo servers proxy; como estas aplicaciones permiten poner components del software en las Firewalls, es el lugar ideal para colocar controles. Por ejemplo, al tener la Firewall la traducción de las direcciones de la red, permite pasar el tráfico en una dirección y no en otra, después que la información pasó por una transacción que realmente enmascaró el origen de la transacción. Al aumentar las prestaciones del Firewall, estas aplicaciones hacen caer el rendimiento notablemente.

En el futuro se esperan desarrollos de Firewalls que combinen ambos niveles, con la velocidad del nivel de red y la flexibilidad del de aplicación.

Con formato: Numeración y viñetas

Con formato: Numeración y viñetas

V.2 Control de Acceso Lógico:

Se puede realizar de distintas maneras:

V.2.1 Por la organización del control

- DAC (Discretionary Acess Control): la autorización de acceso a los objetos la da el creador del archivo. Puede contar con grupos de usuarios o perfiles genéricos, creados por el administrador de Seguridad, para facilitar su tarea.

- MAC (Mandatory Access Control): La administración de Seguridad crea los accesos. Prepara etiquetas (público, secreto bajo nivel, secreto mayor, comercial, etc.) y agrupa los objetos en estas etiquetas. Luego agrupa a los usuarios por función y les asigna los permisos para las etiquetas que correspondan.

- RBAC (Role Based Access Control): trata de combinar los anteriores sin la inseguridad del primero y la rigidez del Segundo. Para ello se exige que se asignen ***roles*** a cada persona en la organización que coincidan con sus funciones, tarea supervisada por la Gerencia. Luego la administración de Seguridad asignará permisos a cada rol.

V.2.2 Por controles por Passwords:

Es el método mas difundido y probablemente el que presente mas debilidades, pero su popularidad se debe a la facilidad de su implementación, aunque se debe tener en cuenta que el usuario deberá enfrentar mayores complicaciones cuando se quiera dotar de mayores seguridades al uso de palabras clave.

Las características básicas de un sistema de passwords eficientes son:

- modificar la password periódicamente en base a la password anterior
- solicitar un número mínimo de caracteres en la password (al menos 8)
- no permitir repetición de caracteres en la passwords
- no permitir reusar passwords anteriores, aunque hayan sido de otros usuarios
- no permitir palabras de diccionario, nombres ni conjugaciones verbales puras
- exigir que las passwords contengan letras, números y signos de puntuación
- que exista un administrador de password que sea el único capaz de acceder y modificar el sistema
- que las passwords se guarden en archivos encriptados, preferentemente por sistema operativo. UNÍX, Windows NT, SQL Server y OS/400 lo hacen así.
- que el administrador cambie sin permiso ni ciclos definidos las passwords del sistema

- que todos los cambios al sistema de passwords queden registrados
- que las passwords usadas en ABM se graben en los registros modificados
- que las passwords para consultas a información sensible tengan el mismo grado de protección que las de actualizaciones.

V. 3 Criptografía:

Es en realidad una rama de las matemáticas muy antigua, que se ha usado para varias aplicaciones, en el pasado principalmente militares y diplomáticas.

Con la aparición de las computadoras se tuvo una herramienta de algoritmación antes imposible de aplicar y además surgió la necesidad de utilizarla para proteger la información de accesos no autorizados.

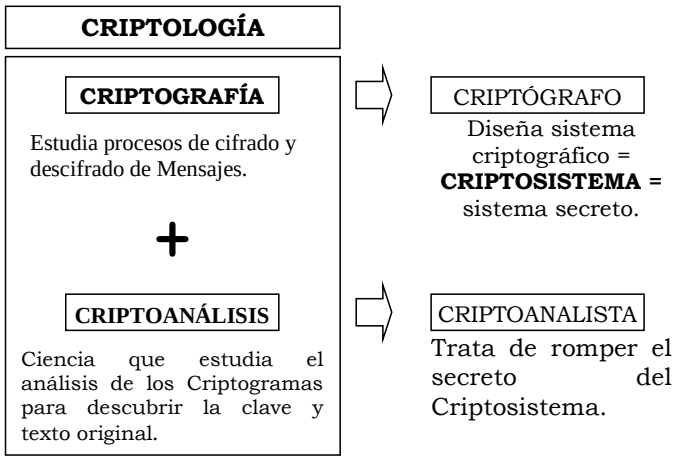
V.3.1 Definiciones:

Por etimología de la palabra:

Kriptos: oculto - Graphos: escribir ⇒ Criptografía ≡ "Escritura Secreta"

V.3.2 Criptosistema, criptograma y criptoanálisis:

CRIPTOGRAMA — Documento cifrado. (CIFRA: escritura secreta).



V.3.3 **Métodos Clásicos:**

- ESCÍTALO LACEDEMONIO**:** Siglo V a.C.

  Utilizaba una cinta con caracteres. Se leía sobre un rodillo.

- CÉSAR: Siglo I a.C.

  Sustituye símbolos del alfabeto según una determinada regla. Sustituye cada símbolo por el que corresponde 3 posiciones a la derecha (X = 3).

0 1 2 **3** 4 5 6 **7** 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 X = 3

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z X = 3

↓

D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

Ejemplo:

Mensaje en claro M: A **U** D I T O RIO
Criptograma C: D **X** G L W R ULR

Mensaje en claro M: E L A U L A E S T A F RIA
Criptograma C: H Ñ D X Ñ D H V W D I ULD

C = (M + 3) mod 27; X = 3

C = (**U** + 3) mod 27 = (21 + 3) mod 27 = 24 mod 27 = 24 = **X**
C = (Y + 3) mod 27 = (25 + 3) mod 27 = 28 mod 27 = 1 = B

- CÉSAR AMPLIADO:

  Se efectúa la sustitución de X posiciones a la derecha; $1 \leq X \leq 26$.

0 1 2 **3** 4 5 6 **7** 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 X = 3

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z X = 3

↓

H I J K L M N Ñ O P Q R S T U V W X Y Z A B C D E F G

Ejemplo:

Mensaje en claro M: L A E C O N O M I A S E C A E
Criptograma C: R H L J V T V S O H Z L J H L

Se pueden agregar caracteres dummy y separadores, con distancias fijas o variables, en función de una progresión en el primer caso y continuos o con interrupción en el segundo.

Por ejemplo: se elimina el carácter W y se lo usa como dummy salteando caracteres en potencias de 2 luego del primer carácter E (el más frecuente en castellano).
Dummy = W
X = 7

Mensaje en claro M: L O S E S T U D I A N T E S N O E S T A N

L O S **E** S W T U W D I A N W T E S N O E S T W A N

2^0 2^1 2^2 2^3

Criptograma C: R V Z L Z D A B D K O H T D A L Z T V L Z A D H T
Es muy vulnerable porque sólo hay 26 claves posibles (desplazamientos). La frecuencia es muy evidente a menos que se usen dummys abundantes y los caracteres siempre se corresponden uno a uno.

- Sustitución Simple Monoalfabeto: Es una variación del César, sustituye cada símbolo por otro según:

  $C = (y \cdot M + x) \bmod 27$

Ejemplo: tomando y = 4 ; x = 10
S = 19
$C = (y \cdot M + x) \bmod 27 = (4 \cdot M + 10) \bmod 27 = (4 \cdot 19 + 10) \bmod 27 = 86 \bmod 27 = 5 = F$

Entonces:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓																										
K	Ñ	R	V	Z	D	H	L	O	S	W	A	E	I	M	P	T	X	B	F	J	N	Q	U	Y	C	G

Es vulnerable como el César pero con mayor dificultad.

- Matricial Simple (Polybios):

Se completan las filas de una matriz con el alfabeto origen y se recorren las columnas para obtener el alfabeto encriptado.

Ejemplo: Matriz de 6x5

A	B	C	D	E
F	G	H	I	J
K	L	M	N	Ñ
O	P	Q	R	S
T	U	V	W	X
Y	Z			

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

↓

A F K O T Y B G L P U Z C H M Q V D I N R W E J N S X

Mensaje en claro M: J U E G A N R I V E R Y B O C A
Criptograma C: P W T B A M I L E T I S F Q K A

- Matricial Con Clave (Polybios con clave):

Igual que el Matricial Simple pero las filas de la matriz se completan primero con una clave y luego con el alfabeto origen. Se hace para que el alfabeto del encriptado no empiece siempre con la letra A. La clave no debe tener letras repetidas ni sus letras deben repetirse en la matriz.

Ejemplo:
- Matriz de 6x5
- Clave: PESCA

P	E	S	C	A
B	D	F	G	H
I	J	K	L	M
N	Ñ	O	Q	R
T	U	V	W	X
Y	Z			

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

↓

P B I N T Y E D J Ñ U Z S F K O V C G L Q W A H M R X

Mensaje en claro M: C A N D E LA
Criptograma C: I P F N T Z P

- Transposición:

Se selecciona una matriz según la longitud del mensaje en claro, con relleno para poder tener una matriz que tenga varios factores. Se rellenan las filas con el mensaje en claro y se lee en las columnas.

Ejemplo 1:

Mensaje en claro M: LA REINGENIERÍA DE PROCESOS ES NECESARIA
Longitud del mensaje = 35
Entonces seleccionamos una matriz de 6x6 con relleno el carácter W.

L	A	R	E	I	N
G	E	N	I	E	R
I	A	D	E	P	R
O	C	E	S	O	S
E	S	N	E	C	E
S	A	R	I	A	**W**

Criptograma C: LGIOESAIACSAREDENRENESEIIEPOCANRRSEW

Ejemplo 2:

Mensaje en claro M: EL RESULTADO DEL PARCIAL ES INCIERTO
Longitud del mensaje = 31
Matriz de 6x6 con relleno el carácter W.

E	L	R	E	S	U
L	T	A	D	O	D
E	L	P	A	R	C
I	A	L	E	S	I
N	C	I	E	R	T
O	**W**	**W**	**W**	**W**	**W**

Criptograma:

C: ELEINOLTLACWRAPLIWEDAEEWSORSRWUDCITW

- Sustitución Homofónica:

Cada símbolo del alfabeto no se sustituye por otro fijo del mismo alfabeto, sino que se sustituye por uno el conjunto de sus símbolos homofónicos. Cada conjunto tiene un número de símbolos proporcional a la frecuencia de aparición de cada símbolo del alfabeto en el idioma, eligiéndose aleatoriamente y teniendo en cuenta que ninguno puede aparecer en más de dos conjuntos. Cuando se realiza la sustitución se puede seleccionar cualquiera de los símbolos del conjunto asociado.

Alfabeto		Conjuntos homofónicos
A	(6)	7, 13, 15, 54, 87, 97
E	(7)	14, 25, 44, 45, 59, 83, 90
G	(2)	56, 89
L	(3)	11, 31, 52
R	(4)	19, 34, 64, 73
U	(3)	5, 39, 61

Mensaje en claro M:	R	E	G	U	L	A
Criptograma C:	19	14	89	39	11	13
ó						
Criptograma C:	34	90	26	5	31	15

- Sustitución Polialfabeto O Vigenere:

Se utiliza más de un alfabeto para el cifrado. Se selecciona una Clave y se arma una matriz tomando las letras de la Clave como partida:

Ejemplo 1:
Clave: LIBRO

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ

Se repite la Clave tantas veces como sea necesario para alcanzar la longitud del Mensaje y se toman las letras de la tabla que se encuentran en la intersección de la columna que empieza con cada letra del Mensaje con la línea que empieza con la letra correspondiente de la Clave:

M =	*L*	*A*	*E*	*N*	*E*	*R*	*G*	*I*	*A*	*D*	*E*	*L*	*U*	*N*	*I*	*V*	*E*	*R*	*S*	*O*
R =	*L*	*I*	*B*	*R*	*O*	*L*	*I*	*B*	*R*	*O*	*L*	*I*	*B*	*R*	*O*	*L*	*I*	*B*	*R*	*O*
C =	*V*	*I*	*F*	*E*	*S*	*C*	*Ñ*	*J*	*R*	*R*	*O*	*S*	*V*	*E*	*W*	*G*	*M*	*S*	*K*	*D*

Se desencripta empezando por las filas con las letras de la Clave, ubicando la intersección de la letra con la columna de la letra en claro.

Ejemplo 2:

Clave: PARIS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R

M =	*S*	*A*	*N*	*T*	*I*	*A*	*G*	*O*	*P*	*E*	*R*	*E*	*Z*
R =	*P*	*A*	*R*	*I*	*S*	*P*	*A*	*R*	*I*	*S*	*P*	*A*	*R*
C =	*I*	*A*	*E*	*B*	*A*	*P*	*G*	*G*	*X*	*W*	*H*	*E*	*Q*

Desventajas:

- Depende del secreto de la clave.
- Si se repiten las ubicaciones de Clave y Mensaje puede dar pistas para descubrirlo.
- Todos los métodos de sustitución se pueden atacar con Diagramas o Trigramas.

◆ Cifrado Vernam o Binario:

Está basado en la generación de una Clave Binaria aleatoria que opera un Mensaje basándose en un OR Exclusivo (XOR). El sistema es absolutamente invulnerable, pero presenta el problema de hacer llegar la Clave al Receptor.

a	b	⊕
0	0	0
0	1	1
1	0	1
1	1	0

M = 1 1 0 1 1 0 0 1
R = 0 1 1 0 1 0 1 0
C = 1 0 1 1 0 0 1 1

- Es completamente aleatorio.
- Es como tener dos Claves (M y R).
- Es el más simple y el mejor de los tradicionales.-

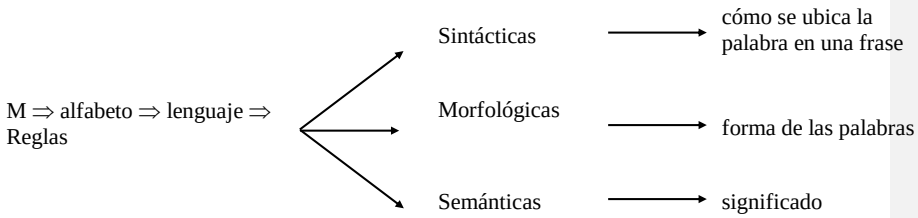
VI : CRIPTOGRAFÍA MODERNA

VI.1 Conceptos Previos:

- **M:** espacio de mensajes

  $M = \{m_1, m_2, \ldots, m_n\}$

  m_i componentes de un mensaje inteligible; pueden ser bits, bytes, caracteres, píxeles, etc., siempre dentro de un determinado alfabeto.



- **C:** espacio de los textos cifrados

  $C = \{c_1, c_2, \ldots, c_3\}$

  Donde se considera que el alfabeto es el mismo para M y C y se supone, en general, que C tiene la misma longitud que M.

- **K:** espacio de claves

  $K = \{k_1, k_2, \ldots, k_n\}$

  Si K tiene la misma longitud que M, estamos ante un "criptograma perfecto".
  K es un conjunto altamente aleatorio de bits, bytes, caracteres, píxeles, etc. que es función de un sistema de cifra o cifrado. Al menos una de las claves se mantendrá en secreto.

- **E_K:** transformaciones de cifrado

  $E_K = M \rightarrow C \quad ; \quad k \in K$

E_K es una aplicación con una clave k incluida en el espacio de claves K que actúa sobre el mensaje M y lo transforma en el criptograma C. Es un algoritmo de cifra puede ser público o secreto.

- **D_K:** transformaciones de descifrado

D_K: C → M ; k ∈ K

D_K es una aplicación con una clave k incluida en el espacio de claves K que actúa sobre el criptograma C y lo transforma en un texto en claro M.

D_K es la inversa de E_K: D_K / E_K

Se suele usar la misma transformación E_K pero con una clave k' que es la inversa de k; k' y k están incluidas en el cuerpo de claves K.

k' / k ; k' y k ∈ K

VI.2 Reglas Generales O Requisitos De Un Criptosistema:

1. El algoritmo de cifrado / descifrado debe ser rápido y confiable.
2. Posibilidad de transmitir archivos y almacenarlos (existen algoritmos que limitan el tamaño de los archivos a transmitir).
3. La seguridad del sistema deberá residir en el secreto de la clave y no en las funciones de cifrado.
4. La fortaleza del sistema se entiende como la imposibilidad computacional de romper la cifra o encontrar la clave secreta.

VI.3 Clasificación De Los Criptosistemas:

sistemas de cifrado ⇨ { Clásicos / Modernos

sistemas de cifrado ⇨ { Bloque (según como se produce el cifrado) / Flujo

De acuerdo al sistema de cifrado se usa una única clave o dos claves (Sistema Privado o Público)

sistemas de clave ⇨ { Secreta o Privada / Pública

FORTALEZA: Tipos de ataques → Criptoanálisis

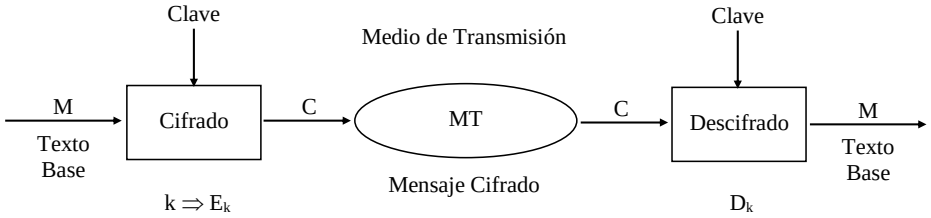
Conociendo el algoritmo de cifrado el criptoanalista intentará romper el cifrado y para ello atacará:

1- Contando únicamente con el criptograma
2- Conociendo un texto en claro M conocido

} descifrado altamente difícil

3- Eligiendo un texto en claro M conocido de antemano
4- A partir de un texto cifrado C elegido
5- Buscando combinaciones de claves aleatorias ("ataque por la fuerza bruta")

VI.4 Criptosistemas De Clave Secreta O Privada:



Lo importante para lograr confidencialidad e integridad es proteger la Clave k.

VI.5 Funciones De Cifrado:

$C = E(M)$
$M = D(C)$

$$M = D(C) = D(E(M))$$

Usando la Clave K:

$C = E(K, M)$
$M = D(K, C)$

$$M = D(K, C) = D(E(K, M))$$

Usando diferentes K:

$$M = D(K_D, E(K_E, M))$$

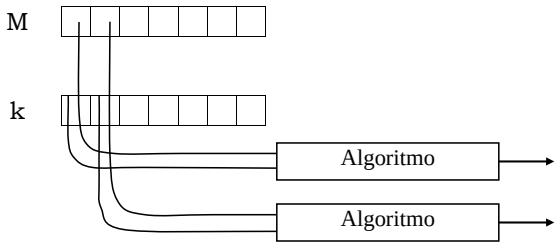
donde D y E son inversas o bien lo son las claves que intervienen, por lo tanto siempre se recupera el mensaje en claro.

VI.6 Cifrado En Bloque Y En Flujo:

- CIFRADO EN BLOQUE:
  El mismo algoritmo de cifrado se aplica a un bloque de información homogéneo (bits, bytes, caracteres, píxeles, etc.) respectivamente, usando la misma clave. Se trata de crear la difusión (permutaciones) y la confusión (sustituciones simples basadas en tablas pequeñas).

  Ventajas:
  - ✓ Alta difusión de los elementos en el criptograma.
  - ✓ Imposibilidad de introducir bloques extraños sin ser detectados.

- CIFRADO EN FLUJO:
  El algoritmo de cifrado se aplica a un elemento de información (bits, bytes, caracteres, píxeles, etc.) mediante un flujo de claves aleatorio y siempre mayor que el mensaje.



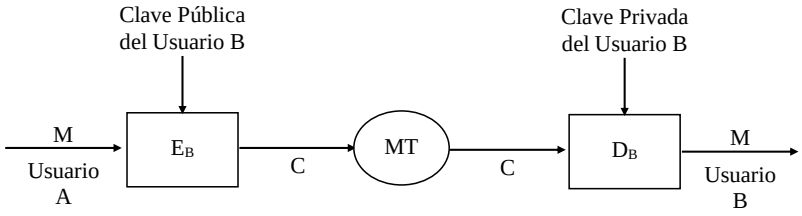
  Al variar el flujo, este cifrado es más seguro.

  Ventajas:
  - ✓ Muy alta velocidad de cifrado ya que no tiene en cuenta otros elementos (control del tamaño del bloque, inicio del bloque, etc.)
  - ✓ Resistencia a errores: cada cifra es independiente para cada elemento.

VI.7 Criptosistemas De Clave Pública:

- CIFRADO Y FIRMA:

- <u>Cifrado:</u>



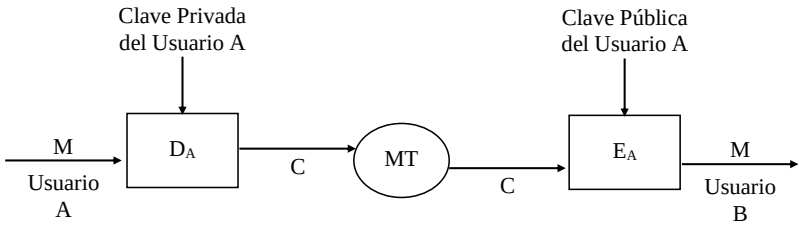
$C = E_B(M) \rightarrow$ Cifrado

$M = D_B(C) = D_B(E_B(M)) \rightarrow$ Descifrado

D_B inversa a E_B

$\Rightarrow$ CONFIDENCIALIDAD

- <u>Firma:</u>



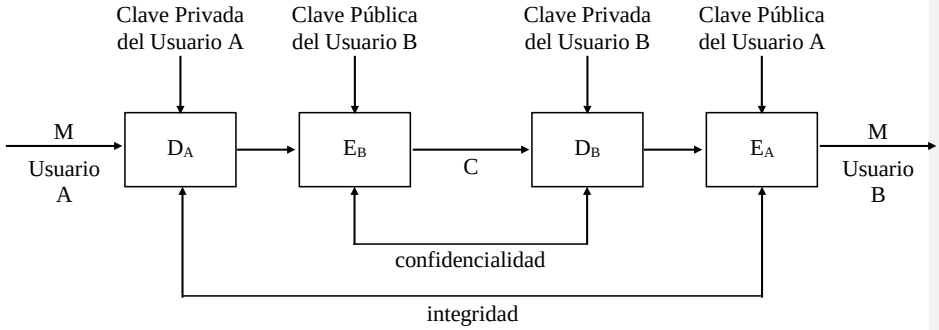
$C = D_A(M) \rightarrow$ Cifrado

$M = E_A(C) = E_A(D_A(M)) \rightarrow$ Descifrado

E_A inversa a D_A

$\Rightarrow$ INTEGRIDAD

- Resumen:

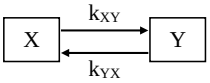


C = E_B (D_A (M)) → Cifrado y firma

M = E_A (D_B (M)) → Descifrado y comprobación de firma

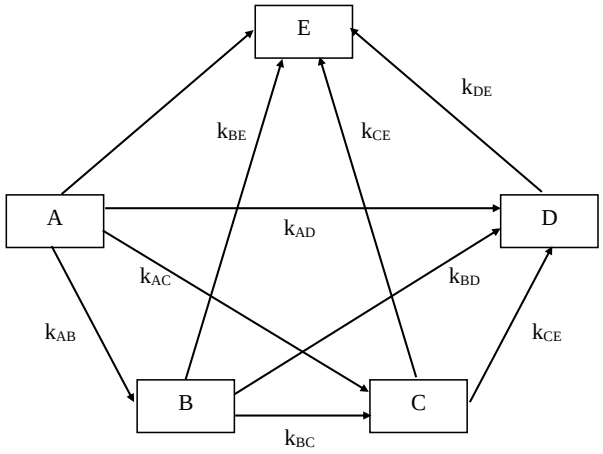
VI.8 El por qué de la Clave Pública:

Porque al tener que obtener la Clave Privada a partir de la Pública existe una mayor cantidad de posibilidades.



N = 10 Claves
U = 5 Usuarios

$$\text{Número de Claves Posibles} = \frac{U\,(U-1)}{2}$$



VI.9 Sistema Lucifer:

Maneja como algoritmo de referencia el ***Algoritmo DES (Data Encryption Standard)***, desarrollado por IBM.

Consiste en un complejo sistema de operaciones matemáticas basado en sustituciones y permutaciones de bits en función de una Clave. Su originalidad es que el conocimiento del algoritmo no permite descifrar la información sin conocer la Clave.

VI.9.1 Cifrado:

El proceso de cifrado trabaja con:

- bloques de 64 bits, y una
- Clave de otros 64 bits (56 bits claves, 8 bits de paridad impar para detección de errores)

- Pasos:

- Se toma el bloque de entrada de 64 bits y se realiza una permutación inicial, conocida como IP, según una determinada tabla fija.
- El bloque resultante se divide en 2 mitades de 32 bits, donde la mitad izquierda se denominará L_0 y la derecha R_0
- A partir de estos 2 bloques se realizan 16 pasos en cada uno de los cuales se efectúa un complejo cálculo que depende de la entrada y de la clave introducida y, al final,
- Se realiza una permutación inversa de la inicial denominada IP^{-1}, cuya salida son los 64 bits cifrados.

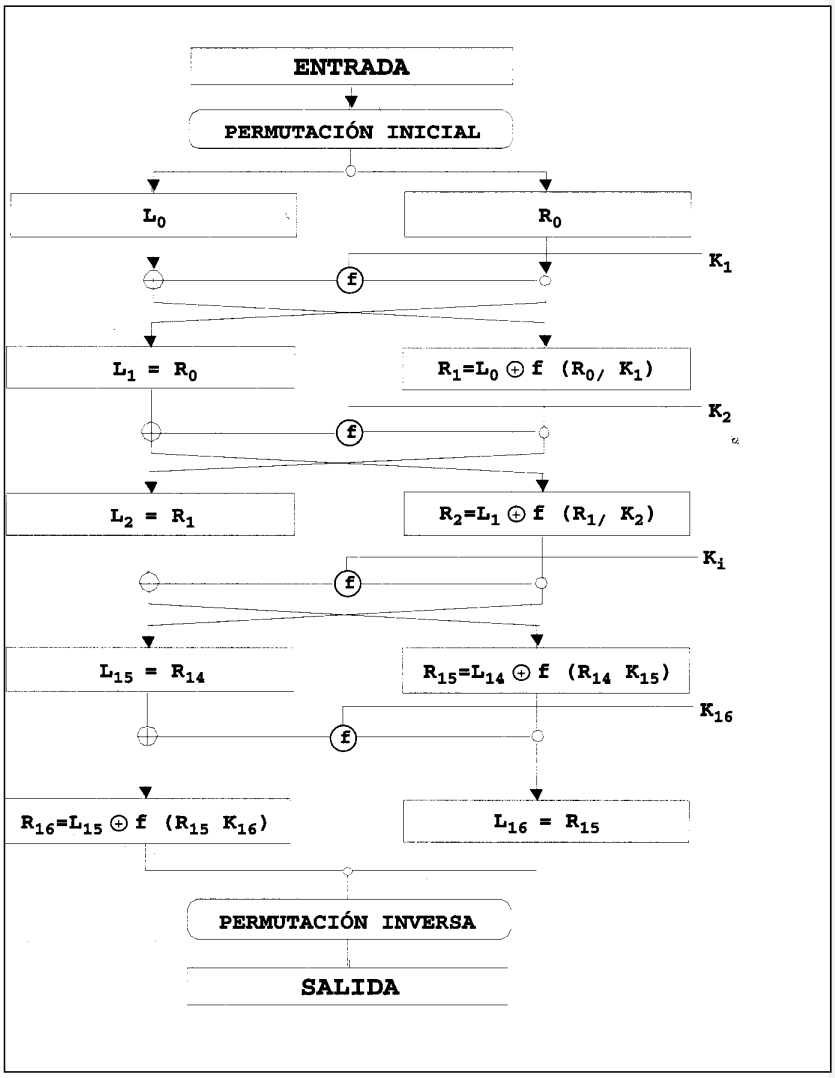
El cálculo que se efectúa en cada paso viene determinado por dos funciones:

- f : función de cifrado.
- KS : función de generación de Claves k_i, cada una de 48 bits, según la cual:

  - $\mathbf{L_i = R_{i-1}}$
  - $\mathbf{R_i = L_{i-1} \oplus f(R_{i-1}, K_i)}$

  donde **i** es el número del paso o iteración que irá desde 1 a 16.

DATA ENCRYPTION STANDARD (DES):



- Se realiza la permutación IP sobre la entrada.
- En el paso 0 se divide el resultado en 2 bloques L_0 y R_0.
- En L_1 queda el bloque R_0 del paso anterior, en R_1 queda el resultado de aplicar L_0 y el $\oplus$ del valor devuelto por la función f, cuyos parámetros son R_0 y el valor devuelto por la función de generación de Claves KS.

- En los siguientes pasos hasta el 16, se aplican las mismas expresiones, pero en el último paso, en el bloque izquierdo queda R_{16} y en el derecho L_{16}.
- Finalmente se hace la permutación inversa IP^{-1}.

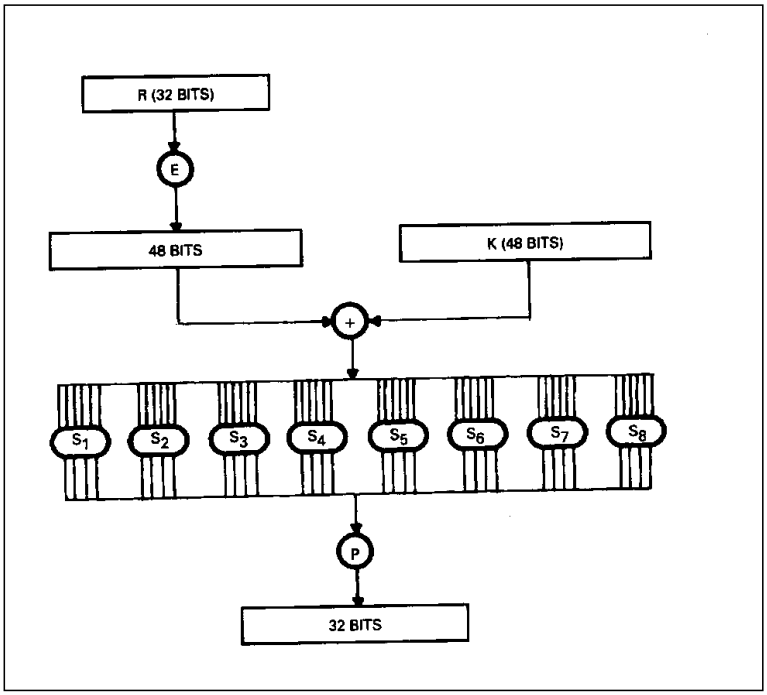
VI.9.2 Funciones IP e IP-1:

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP - 1							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

VI.9.3 Función De Cifrado f: $f(R_{i-1}, K_i)$

Recibe dos parámetros: R_{i-1} y K_i, el primero de 32 bits y el otro de 48 bits, y su salida es un bloque de 32 bits.



La función E de expansión recibe un bloque de 32 bits y produce uno de 48 bits consistente en una permutación de los bits de entrada repitiéndose 16 de ellos según la siguiente tabla, donde los valores indican la posición de los bits de entrada:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Con la salida de la función E se realiza una operación o - exclusiva con K_i, y el resultado, que será también un bloque de 48 bits, se divide en ocho grupos de 6 bits. Estos ocho grupos serán las entradas de las funciones S_i también llamadas cajas.

Las funciones S_i reciben un bloque de 6 bits y devuelven uno de 4 bits; por tanto, los 48 bits totales de entrada a las ocho funciones S_i se convierten en 32 bits a la salida. Los pasos que se llevan a cabo en esta función son: se toman los bits 2, 3, 4 y 5 del bloque de entrada y al valor que forman (comprendido entre 0 y 15), se le denomina x; después se toman los bits 1 y 6 denominándose y al valor que forman (comprendido entre 0 y 3).

Los valores de x e y se utilizan como coordenadas de columna y fila para extraer los valores de una tabla de 16 columnas (0-15) por 4 filas (0-3). Existe una tabla distinta para cada S_i; es decir, ocho tablas numeradas de S_1 a S_8.

Ejemplo:

x / y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Los valores de la tabla están comprendidos entre 0 y 15, por tanto son valores de 4 bits que devolverá cada función S_i.

Para finalizar, a los 32 bits obtenidos como salida de las ocho funciones S_i se les somete a una permutación en la que se reordenan sus bits de la siguiente forma:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

VI.9.4 Función De Generación De Claves Ks:

Esta función devuelve las claves K_i utilizadas en la función f, $f(R_{i-1}, K_i)$ siendo su entrada la clave de cifrado de 64 bits.

En primer lugar, efectúa una permutación de los bits de la clave de cifrado denominada PC-1 en la que también se eliminan los 8 bits de las posiciones múltiplo de 8, que corresponden al bit de paridad. Dicha permutación es la siguiente:

P C - 1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Los 56 bits resultantes se dividen en dos mitades, denominadas C y D, y sobre cada mitad de 28 bits se realiza una rotación a la izquierda de un determinado número de bits en función del paso que se trate, según la siguiente tabla:

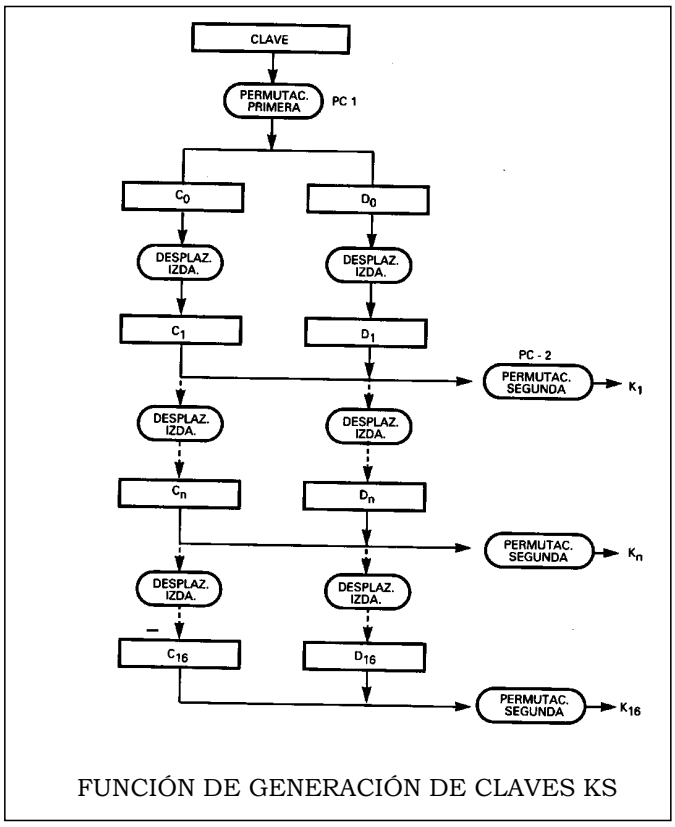
Nº paso	Nº de bits a rotar
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Primero se efectúa la permutación inicial (PC-1) sobre la clave de entrada, después se divide el resultado anterior en dos bloques que son la mitad izquierda (C_0) y la mitad derecha (D_0) de la entrad permutada.

A partir de estos dos bloques, se empiezan a realizar las rotaciones a la izquierda según indica la tabla anterior, de tal forma que C_1 y D_1 se obtienen realizando la rotación de 1 bit a la izquierda sobre C_0 y D_0. C_3 y D_0 se obtendrán efectuando una rotación de 2 bits a la izquierda sobre C_2 y D_2 y así sucesivamente.

Al final de cada paso se realiza una permutación denominada PC-2, en la que se eliminan 8 bits más siendo, por tanto, su salida un bloque de 48 bits, que corresponderá a cada una de las utilizadas en la función f.

P C - 2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32



FUNCIÓN DE GENERACIÓN DE CLAVES KS

VI.9.5 Descifrado:

Se realiza con el mismo algoritmo utilizado para el cifrado pero teniendo en cuenta que tras la permutación inicial se partirá de los bloques R_{16} y L_{16} siendo $L_0 R_0$, los bloques obtenidos en el último paso. La primera clave que utilizará la función f será K_{16} y la última K_1 por tanto, las expresiones que definen el cálculo realizado en cada paso serán las siguientes:

- $\mathbf{R}_{i-1} = \mathbf{L}_i$
- $\mathbf{L}_{i-1} = \mathbf{R}_i \oplus \mathbf{f}(\mathbf{L}_i, \mathbf{K}_i)$

VI.9.6 Seguridad Del Algoritmo:

La única forma conocida de violar el algoritmo es probar a descifrar la información con todas las posibles claves. Puesto que constan de 56 bits habría que probar con 256, es decir, 7.057.594.037.927.936 claves distintas. Suponiendo que se dispone de un ordenador de gran potencia capaz de generar y probar un millón de claves por segundo, se requerirían unos 72.000 millones de segundos (2.285 años). Sin embargo, utilizando un superordenador con multitud de procesadores en paralelo, se podrían generar todas las claves en tan sólo horas, aunque este tipo de ordenadores no está al alcance de cualquiera.
Actualmente se utiliza un algoritmo derivado del DES: IDEA. Duplica el tamaño de la Clave (128) y se realizan 3 cifrados por cada bit (3 veces todas las operaciones).

VI.10 RSA (RIVEST - SHAMIR - ADLEMAN):

Se basa en un algoritmo que se construye a través de los factores primos de los grandes números.

a. Se eligen 2 números primos grandes tal que: $n = p \cdot q$

b. Se escoge un número que no tenga divisor común (aparte de 1) d en el rango $2..n-1$:

d / MCD $(d, (p-1) \cdot (q-1)) = 1$

$p, q > d$

c. Se calcula un número e:

e / $e \cdot d = 1 \pmod{((p-1) \cdot (q-1))} \equiv (e \cdot d) \bmod ((p-1) \cdot (q-1)) = 1 \equiv \frac{e \cdot d}{(p-1).(q-1)} \Rightarrow$

resto 1

$\therefore$ e *inversa* (d, (p - *1)*(q - *1))*

inversa e => *e.d mód (p-1).(q-1)*

d. Se publican los valores e y n, ambos forman la Clave Pública, mientras d permanece secreto, ya que d junto con n forman la Clave Privada de cada usuario y por lo tanto, p y q también deben permanecer secretos.

Para enviar la información:

$C = M^e \bmod n$

- M puede estar en código ASCII

- n debe ser mayor que el valor máximo de cada bloque que se transmita, por lo tanto, si se usa la tabla ASCII, $n > 256$.

Se agrupan todos los bloques de igual tamaño y para cada uno de ellos se aplica:

$$C_1 = M_1^e \bmod n$$
$$C_2 = M_2^e \bmod n$$
$$\dots$$

Se envía el conjunto de la información cifrada:

$$C = C_1, C_2, C_3, \cdots C_n$$

Para descifrar el Receptor usará:

$$M = C^d \bmod n$$

o sea que por cada bloque recibido será:

$$M_1 = C_1^d \bmod n$$
$$M_2 = C_2^d \bmod n \ \dots$$

Ejemplo:

Emisor	*Receptor*
	▪ Elige: p = 17; q = 23 ⇒ $n = p \,.\, q$ = 17 . 23 = 391 ▪ Elige d = 15 / (p - 1) . (q - 1) = 16 . 22 = 352 MCD(d, (p-1).(q - 1)) = MCD (15, 352) = 1 p = 17; q = 23 > d = 15 y d = 15 < n = 391 ▪ Calcula e: e . d mod *(p-1).(q-1)* = e . 15 mod 352 = 1 e = inversa (15, 352) = 47 Comprobación: 47 . 15 mod 352 = 705 mod 352 = 1 ▪ Publica (e = 47, n = 391) => Clave Pública (d = 15 , n = 391) forman la Clave Privada

- Selecciona M = AGUJERO

  En ASCII:
  97 103 117 106 108 114 111

- Aplica la función de Cifrado:

  $C_1 = 97^{47} \bmod 391 = 10$
  $C_2 = 103^{47} \bmod 391 = 273$
  $C_3 = 117^{47} \bmod 391 = 8$
  $C_4 = 106^{47} \bmod 391 = 30$
  $C_5 = 101^{47} \bmod 391 = 16$
  $C_6 = 114^{47} \bmod 391 = 367$
  $C_7 = 111^{47} \bmod 391 = 189$

- Aplica la función de Descifrado:

  $M = C_1{}^d \bmod n$
  $M_1 = 10^{15} \bmod 391 = 97$
  $M_2 = 273^{15} \bmod 391 = 103$

VI.11 Seguridad Del Algoritmo:

Radica en el tamaño de *n*. El mínimo a transmitir con seguridad es de 512 bits, para una alta seguridad se utilizan 1024 bits. Por ejemplo: con un supercomputador para 300 dígitos hacen falta 1,5 x 10^{29} operaciones, por lo tanto para la factorización se necesitan 4.800 billones de años para un computador que resuelva operaciones por nanosegundo.

VI.12 Otras Aplicaciones:

El algoritmo RSA da origen a varias aplicaciones de uso común, no sólo para la transmisión de información sino para asegurar el almacenamiento de los sistemas en producción.

Sobre su base, existe el PGP (Pretty God Privacity), que se combina con un sistema de Firma Digital (Diffie – Hellmann), dando un algoritmo de alto nivel de seguridad y fácil uso, incluso obtenible desde Internet.

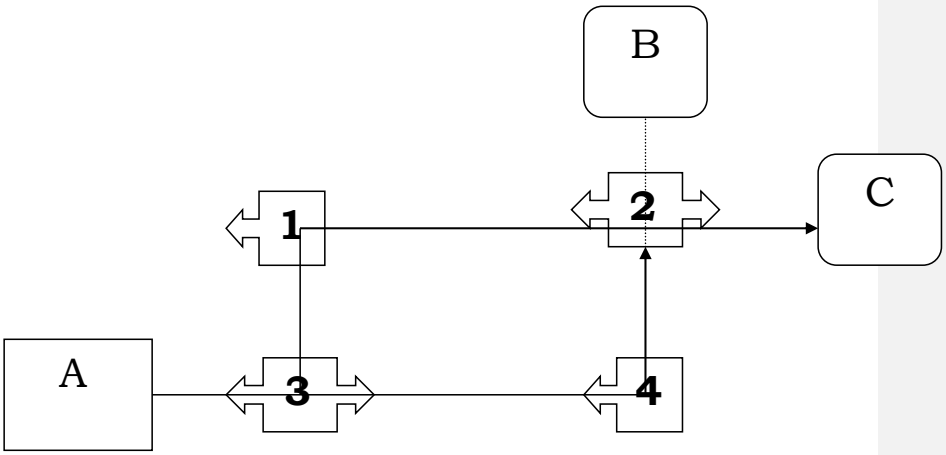
Para mayores niveles de seguridad, se usa el algoritmo de El Gammal, que en lugar usar la lógica de los módulos n se basa en curvas elípticas, donde la dificultad radica en calcular el logaritmo discreto de un número en ese entorno, en lugar de la imposibilidad de factorizar un número o calcular raíces é-simas como en los casos antedichos.

VI.13 <u>Criptografía Cuántica:</u>

Basada en un fenómeno físico de reflectancia de la luz que se está estudiando hace pocos años; promete cambiar totalmente el concepto del criptoanálisis, sino el de la Informática toda.

En el ejemplo siguiente, se supondría que los receptores ***B*** y ***C*** serían excitados por los fotones con una probabilidad de un 50% cada uno. Sin embargo, al realizarse la experiencia se comprueba que ***B*** no detecta nada.

A : emisor de fotones
B y C : receptores sensibles
1 y 4 : espejos totalmente reflectantes
2 y 3 : espejos que reflejan la mitad de la luz que reciben y dejan pasar la otra mitad

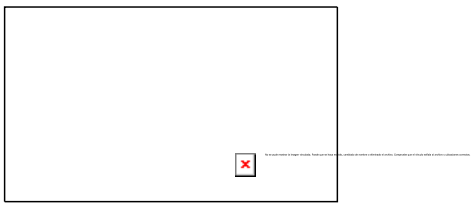


Esto significa que, a nivel subatómico (donde trabaja la Física Cuántica), una partícula puede estar en dos sitios simultáneamente, o, dicho de otra forma, con la superposición cuántica de dos estados.

Si se construye un dispositivo capaz de representar bits mediante estados cuánticos de una o muy pocas partículas que son colocadas en los dos estados básicos, se tendría un ***bit cuántico o qubit*** que puede representar los estados 0 y 1 al mismo tiempo.

El qubit (quantum bit por sus siglas en inglés), representa ambos estados simultáneamente, un "0" y un "1" lógico, dos estados ortogonales de una sub partícula atómica, como es representada en la figura 1. El estado de un qubit se puede escribir como { ½ 0ñ , ½ 1ñ } , describiendo su múltiple estado simultaneo.

Un vector de dos qubits, representa simultáneamente, los estados 00, 01, 10 y 11; un vector de tres qubits, representa simultáneamente, los estados 000, 001, 010, 011, 100, 101, 110, y 111; y así sucesivamente. Es decir un vector de n qubits, representa a la vez 2^n estados.



Los ordenadores cuánticos tendrían sus propias formas de representar, guardar, copiar y operar qubits. Igual que ocurre con los bits, la forma exacta en que hagan estas cosas no es demasiado importante, y sería absurdo intentar adivinar ahora qué tecnologías se usarán en el futuro. Hasta ahora se han usado iones atrapados en campos eléctricos dentro de cámaras de vacío a temperaturas bajísimas; estos iones se pueden manipular con láseres. En otros casos, cada qubit se ha representado con el spin de un electrón atrapado en un pozo cuántico, de forma que si "giraba" en un sentido representaba un 1 y si giraba en el sentido contrario representaba un 0. En estos casos el valor el qubit se puede manipular con campos magnéticos.

Esto permitiría factorizar a una velocidad impensable con los métodos actuales y por lo tanto caerían la mayoría de los algoritmos criptográficos actuales que basan la dificultad de sus ataques en el tiempo que insume al computador la factorización de grandes números.

Hasta el momento no se ha conseguido fabricar un procesador que pueda mantener estables las partículas cuánticas que lo integrarían, pero ya existen algoritmos para emplear los qubits como elementos de cálculo.-

IV : AUTENTIFICACIÓN Y ESTEGANOGRAFÍA

Los métodos de autentificación se utilizan para asegurar la integridad de los mensajes transmitidos. Aun cuando éstos estén encriptados y el atacante no pueda interpretarlos, puede agregar o quitar caracteres de manera de afectar el contenido.

Estos métodos se usan actualmente en la Argentina, por ejemplo en el sistema Osiris de la D.G.I. y en muchos sistemas bancarios privados, de manera de dar una alta seguridad a las transacciones vía Internet o por otras redes.

VII FIRMA DIGITAL:

La firma digital se utiliza para certificar un documento por medio de la transmisión de un criptograma que contiene una identificación del emisor junto con una función resumen, también conocida como MDC (Modification Detection Code) tal que $E_{Kp}\,(r(m))$, donde:

- *r(m)* es de longitud fija, independientemente de los valores que resuma y de la longitud del mensaje *m*
- *m* permite calcular fácilmente *r(m)* si se utilizó la clave privada *Kp* para encriptarlo y se utiliza la correspondiente clave pública para desencriptarlo
- dado un *r(m)*, es computacionalmente intratable calcular *m*
- dado un *m*, es computacionalmente intratable obtener un *m'*, tal que *r(m) = r(m')*

Existen varios métodos de aplicación, aunque en general se pueden usar los mismos que para encriptar en clave asimétrica, entre ellos el DSS (Digital Signature Standard), RSA y el PGP (Pretty Good Privacy), de uso gratuito.

En general, se usan sistemas de clave simétrica para transmisión de mensajes largos y los de asimétrica para las firmas digitales, ya que estos bajan mucho la perfomance de la operación por la cantidad de información adicional que llevan y su operación algorítmica mas compleja.

Ejemplo:

Privada $\begin{cases} d \\ n \end{cases}$ $\Rightarrow S = M^d \bmod n$

Pública $\begin{cases} e \\ n \end{cases}$ $\Rightarrow M = S^e \bmod n$

Por tanto, si el emisor A de Clave Pública (e_a, n_a) y Clave Privada (d_a, n_a) quiere enviarle un Mensaje a B de Clave Pública (e_b, n_b) y Clave Privada (d_b, n_b), seguirá el siguiente proceso:

- A firma con su Clave Privada y cifra con la Clave Pública de B:

  $S = M^{dA} \bmod n_A$

  $C = S^{eB} \bmod n_B$

- B descifra y verifica con su Clave Privada y la Clave Pública de A:

  $S = C^{dB} \bmod n_B$

  $M = S^{eA} \bmod n_A$

Lo cual garantiza a B que el mensaje proviene de A.

VII.1 DIFFIE - HELLMAN (D - H):

Es muy seguro, aunque se intercepte no puede ser descifrado.

Se elige:

- primo p
- entero g

} públicos

Siendo dos usuarios A y B que desean tener una clave en común: A elige un número a y B un número b, tal que a y b sean enteros positivos (secretos).

- A → a
- B → b

} enteros positivos

Se calcula:

- para A: $X_A = g^a \bmod p$
- para B: $X_B = g^b \bmod p$

$X_B{}^a = (g^b \bmod p)^a = g^{ab} \bmod p$

y se intercambian los valores obtenidos:

- A $\xrightarrow{X_A}$ B
- B $\xrightarrow{X_B}$ A

Se calcula:

- para A: $Y_A = X_B^a \mod p$
- para B: $Y_B = X_A^b \mod p$

Reemplazando:

- $Y_A = g^{ab} \mod p$
- $Y_B = g^{ab} \mod p$

$Y_A = Y_B = K \Rightarrow$ A y B tienen la misma clave.

VII.1.1 <u>Cifrado:</u>

$C = M^K \bmod p$

VII.1.2 <u>Descifrado:</u>

Se calcula: $K^{-1} \Rightarrow$ MCD $\begin{matrix} p-1 \\ K \end{matrix}$

que multiplicado por el mod *(p-1)* implica:

$K^{-1} = \text{MCD}\ ((p-1).K) \bmod (p-1)$

Verificación: $K \cdot K^{-1} = 1 \bmod p - 1$

Ejemplo:

$p = 11$;
$g = 2$;
$a = 8$;
$b = 11$;
M = 9

A	B
$Y_A = g^a \mod p$	$Y_B = g^b \mod p$
$Y_A = 2^8 \mod 11$	$Y_B = 2^{11} \mod 11$
$Y_A = 3$ →	← $Y_B = 2$
← $Y_B = 2$	$Y_A = 3$ →
$K = Y_B^a \mod p$	$K = Y_B^a \mod p$
$K = 2^8 \mod 11$	$K = 3^{11} \mod 11$
K = 3	K = 3

$\therefore Y_A = Y_B$

$C = M^K \bmod p = 9^3 \bmod 11 = 3$

VII.1.3 Cálculo de K^{-1} (por Euclides): *$K^{-1} = MCD((p-1),K) \bmod (p-1)$*

MCD $p-1$	10	0	3
K	3	1	3
	1	-3	
	0		

$K^{-1} = -3 \bmod 10$

$K^{-1} = 7$

Verificación:

$K \cdot K^{-1} = 1 \bmod p - 1$
$21 = 1 \bmod 10 \Rightarrow 1 = 21 \bmod 10$
$1 = 1$

$$M = C^{K-1} \bmod p = 3^7 \bmod 11 = 2187 \bmod 11 = 9$$

VII.2 CERTIFICADO DIGITAL

La idea básica es poseer una clave pública y un identificador con firma digital de una autoridad de certificación que avale al emisor.

Existen varias normas y métodos; uno de los mas difundidos es la Certificación X – 509; la misma se usa en forma standard sobre todo en el sistema financiero.

Contiene una serie de campos que son fijos para cualquier transmisión:

- Versión
- Nº de serie
- Identificación del algoritmo empleado para la firma digital
- Nombre del certificador
- Período de validez
- Nombre del sujeto
- Clave pública del sujeto
- Identificador único del certificador
- Identificador único del sujeto
- Extensión del mensaje
- Firma digital

Estos Certificados se envían con una estructura jerárquica, de manera de asegurar una escala de seguridades de acuerdo al nivel del certificador.

Nunca se debe aceptar el envío de otra clave que no sea la pública, debiendo la autoridad de certificación autorizar con su identificador luego de un acuerdo con el emisor.

VII.3 Esteganografía:

Se basa en conseguir ocultar un archivo de datos dentro de una imagen; el objetivo es obtener una imagen final, que en

apariencia fuese idéntica a la inicial pero que en su interior albergase información oculta. Existen programas que tratan de conseguirlo, el mas famoso se llama Camuflage, que añade información al archivo, encriptandola, pero modificando la estructura de la imagen.

Otros, como el ***Algoritmo 8t3,*** basado en el estudio de criptología de Bruce Schneier, y más en concreto en su algoritmo Blowfish, permite ocultar una cierta cantidad de información en una imagen, pero sin modificar la estructura, ni haciendo que esta aumente de tamaño. Obviamente la cantidad de información a ocultar esta limitada, pero a cambio obtenemos un archivo que no tiene ninguna referencia que le distinga de las demás imágenes.

La base del algoritmo es la codificación basada en a-8t3 (Blowfish) la cual es un sistema simple pero factible; consiste en fragmentar un byte en tres bloques de bits de tal manera que estos bloques se reparten en otros tres bytes. Los tres últimos bytes a los que hacemos referencia son los bytes de un bloque de datos que contiene información que puede degradarse o modificarse sin que ello perjudique el resultado final de la información misma.

Si se toma una imagen de 100x100 pixels y 24 bits de color, esto significa que el mapa esta compuesto por 10000 pixels que ocuparan 30000 bytes (3 bytes por pixel). Cada uno de los bytes se corresponde con el rojo, verde y azul de la triada de color.

1 pixel = > 3 bytes

1	byte	de	rojos	(0-255)
1	byte	de	verdes	(0-255)
1	byte	de	azules	(0-255)

total = 24 bits de información por pixel.

La aplicación sería la siguiente: tomando un byte de la información que se desea ocultar, se fragmenta en 3 bloques, dos de 3 bits y uno de 2 bits (que suman 8 bits). Transferimos esos grupos a cada uno de los bytes que compone el pixel. En el ***Anexo 3*** hay un ejemplo de imagen.

Realizando esta operación con los sucesivos bytes de información, aplicándolos sobre cada pixel del mapa de la imagen original

obtendríamos una fotografía final de 24 bits idéntica en un 100% con una cromaticidad próxima al 67% de la original (correspondiente a una imagen de 16bits de color). El ojo humano no lo notará en absoluto.

Esa imagen que a vista humana es normal y corriente tendrá integrada en su propia información los datos que se han ocultado. Este algoritmo no sólo puede ser aplicado a imágenes, también puede aplicarse a sonidos.

Como limitaciones del algoritmo se debe mencionar que si la imagen sufriese una adulteración la información se vería gravemente dañada. Asimismo la capacidad de la imagen utilizada para almacenar la información es limitada.-

VIII : VIRUS INFORMÁTICOS

Un virus informático es un programa o conjunto de programas creados para dañar a quien los use y cuya principal habilidad es la replicación. Su acción va desde una broma hasta la destrucción total o la confusión de la información, pasando por la intrusión remota en los archivos del computador vía Internet.

- 1985 -> 25 virus
- 1995 -> 8000 virus
- 2000 -> 12.000 virus, aumentando a razón de 10 por día

Es imposible determinar la magnitud del daño que producen los virus informáticos, pero algunos datos pueden dar idea de su magnitud:

- En 1996 se produjeron pérdidas por U$S 2.000.000.000.

- En enero del 2003 un solo virus afectó todos los e-mail de Estados Unidos, habiéndose perdido el 20% del total de los enviados en un día, con un volumen de información y dinero perdidos difícil de calcular.

- En Enero de 2004 un solo virus destruyo 1 / 3 de todos los e-mail enviados en un día en Estados Unidos; el mismo día otro (o el mismo, no se sabe aún) destruyo todos los sites de SCO en Internet.

Los daños van desde la reducción de la performance del equipo hasta la destrucción de archivos, siendo los más graves los que cambian datos sin rastros del proceso (por ejemplo: cambio de un número).
Su función inicial fue proteger de los derechos de autor contra las copias de software no autorizadas. Los beneficiados actuales son muchos, pudiendo nombrarse los que reparan los daños de los virus, los que producen virus (hackers) y los que desarrollan antivirus; ello se ve facilitado con la existencia de mas de 35.000 web sites para hacking en Internet.

VIII.1 PRINCIPALES TIPOS DE DAÑOS:

- Modificar programas para que funcionen erróneamente o dejen de funcionar

- Modificar datos en bases de datos y archivos convencionales

- Eliminar fisicamente programas y archivos, incluso por formateo del disco
- Ocupar el espacio libre en disco para producir un system crash por falta de espacio
- Perjudicar la perfomance del sistema, llegando a hacerlo inoperante
- Robar información confidencial
- Bloquear la autorización de accesos
- Borrar el BIOS
- Quemar el procesador por introducción de falsa información en el sensor de temperatura
- Rotura de los mecanismos de brazo del disco rígido por la repetición forzada de lectura de determinadas pistas
- Ingresar a un equipo remoto y comandarlo

VIII.2 INDICADORES DE PRESENCIA:

- El programa crece indefinidamente.
- Cambian las fechas de los archivos.
- El acceso al HD da más errores que lo habitual.
- El número de sectores dañados del disco aumenta demasiado.
- Los comandos del SO parecen correr más lentamente.
- La RAM libre se vuelve más pequeña que lo habitual.
- Los programas residentes en RAM no responden o lo hacen con errores.
- El equipo no responde al teclado.
- El HD trabaja sin razón aparente.

VIII.3 <u>CLASIFICACIÓN:</u>

SHELL (caparazón) o WORM (gusano)	Consiste en envolver el programa residente sin modificarlo. Por ejemplo crean una rutina que cuenta hasta una determinada cifra, varias veces, esta se copia indefinidamente hasta desbordar la RAM. Son los más antiguos, los más simples y los más abundantes. Sólo atacan programas ejecutables: Fáciles de detectar y remover. (Por ejemplo el Norton Antivirus compara el tamaño del programa en memoria y el tamaño que previamente guardó).
INTRUSIVOS o PUROS	Invaden un programa existente insertando una parte de su código dentro del programa anfitrión. Son altamente corruptivos porque se instalan en memoria y desde allí se activan al detectar la ejecución de un determinado código del anfitrión, de manera que la infección es transparente al usuario. Fáciles de detectar, difíciles de remover.
DE SISTEMAS OPERATIVOS o DE BOOTEO	Reemplazan parte del SO con su propia lógica. Son pocos y muy difíciles de escribir, muy peligrosos porque asumen el control en el momento de arranque. Utilizan sectores de disco falsamente marcados como inutilizables donde almacenan gran cantidad de código. <u>La única forma de eliminarlos es formateando el disco.</u>
DE CÓDIGO FUENTE	Se instalan en programas residentes de la RAM o en drivers de dispositivos para infectar los sistemas elegidos. Son fáciles de eliminar pero difíciles de detectar porque se confunden con una falla física.
TROYANOS	Son programas completos que se ocultan en otros programas del sistema y producen sus efectos cuando éste se ejecuta. No infecta otros archivos y se ejecuta sólo una vez soliendo tener alto efecto destructivo. Muy difíciles de detectar y suelen estar preparados para efectuar todo el daño de una sola vez.
CAMALEONES	Son similares a los Troyanos, actuando como un programa del usuario al cual copia e imita en todas sus funciones, aunque en realidad agrega funciones que permiten la piratería, como registrar passwords y luego enviarlas a un usuario no autorizado.

AGENTES ACTIVOS	Son programas en JAVA que se graban en el disco rígido cuando el usuario está conectado a Internet y se ejecutan al navegar una determinada página. Pueden afectar cualquier área de la PC e incluso enviar mensajes desconocidos por el usuario a un sitio WEB.
De HTML	Están en páginas WEB en archivos HTML y se activan con sólo conectarse a la página. Sólo puede atacar a versiones Windows 98 o superiores. Generalmente borran o alteran archivos del disco rígido.
FALSOS O HOAX	Son falsas alarmas de virus; persiguen saturar los servidores, sobre todo de e-mails, con mensajes de advertencia. También solicitan respuestas que tienen como objeto levantar direcciones de e-mail para luego enviar publicidades no deseadas o realizar Spamming.
MACROVIRUS	Son aquellos virus escritos en macros de los utilitarios. Sólo pueden afectar al documento en que se encuentran. Fáciles de hacer, difíciles de detectar y de daño moderado. Suelen difundirse por Internet.
BOMBA LÓGICA	Son programas que se activan cuando se produce una acción concreta del SO, predeterminada por el creador.
MUTANTES o POLIMÓRFICOS	Son los más peligrosos. Su diseño les permite asumir nuevas funciones a medida que se van distribuyendo. Se autoencriptan, cambian por sí mismo la clave de encripción. No se los puede contrarrestar ya que no se pueden leer.

VIII.4 ESTRATEGIAS MAS COMUNES PARA INSTALAR VIRUS:

Estas técnicas están en permanente evolución y creación, y dado su carácter secreto es difícil mantener su conocimiento actualizado.

- Sustitución: reemplaza directamente el código anfitrión por el del virus; al ejecutarse reporta algún tipo de error para disimular la no ejecución del programa original. Es el mas simple de realizar pero en general se puede ejecutar una única vez sin que el usuario se aperciba.

- Agregado: se agrega al final del archivo a infectar las rutinas del virus, cambiando el código de arranque del programa de manera que ejecute primero la rutina de virus, realizando su tarea intrusiva y

luego entregando el control al programa para que sea mas difícil de detectar, aunque invariablemente aumenta el tamaño del archivo.

- Inserción: la rutina del virus se aloja en segmentos del archivo no utilizados o reemplaza algunos de poca utilización, prosiguiendo luego igual que el Agregado pero con la ventaja para él de no aumentar el tamaño. No se usa mucho por la gran dificultad de codificación que implica.

- Redireccionamiento: como variante de la inserción, las rutinas de virus se colocan en sectores de disco marcados como defectuosos, intercalando trozos pequeños de código en segmentos del programa principal que dirijan el control a las rutinas.

- Polimorfismo: se introduce la rutina en el programa anfitrión, pero para evitar el aumento de tamaño se compactan partes del código propio y del anfitrión, igualando en la suma del tamaño al original del archivo. Al ejecutarse el programa, primero descompacta y luego ejecuta la rutina intrusiva. Es el método mas avanzado y requiere un nivel medio de dominio de la programación.

VIII.5 TÉRMINOS Y TÉCNICAS DE LOS HACKERS:

- Eavesdropping (atacar desde arriba)*:*
  Se trata de una intervención pasiva sobre un tráfico de red pero sin modificación de mensajes. Para ello utilizan los Packet Sniffers, que son programas que monitorean los paquetes de red direccionados a un equipo especial:
  - Estación de trabajo
  - Host o server
  - Router
  - Gateway

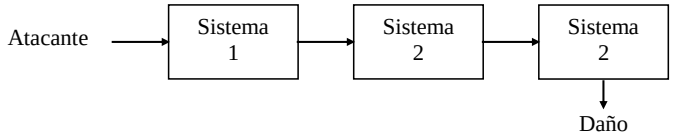
  Intentan robar:
  - passwords
  - números de tarjetas de crédito
  - direcciones de e-mail

- Snooping (snoop = entrometerse) :
  Tiene el mismo objetivo que el Sniffing, pero además de obtener passwords y direcciones toma documentos completos y realiza downloads.

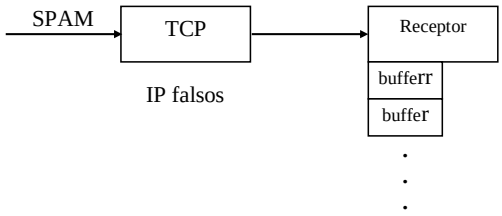
- Tampering (tamper = inmiscuirse) o Data Diddling (diddl = engaño)*:*

Se refiere a la modificación no autorizada de datos o de software instalado. Es el medio preferido de los Hackers Insiders. Suelen ser empleados de bancos o entidades financieras que utilizan el Tampering para crear cuentas falsas y transferir fondos a otras cuentas.

- Spoofing (spoof = estafador):
  Es una técnica que permite actuar en nombre de otros usuarios. Se comienza con la password de un usuario para que, una vez dentro del sistema, envíe o dispare comandos en su nombre. Lo más común es usar un Looping permitiendo perder la pista del atacante:



- Jamming (enredar) o Flooding (mezclar):
  Se utiliza para saturar los sistemas. Por ejemplo mandando un mensaje SPAM a través de un TCP, pero usando IP falsos a los cuales el Receptor trata de responder.



- PING De La Muerte: PING es un mandato utilizado con una red Windows que produce la generación de una serie de caracteres que establece una conexión, indicándola con un sonido de campana. El Ping de la muerte se logra cambiando un carácter del mandato Ping que produce la orden reboot de la red. Una variante de este es enviar una gran cantidad de trabajos en lugar de los blancos que usa este mensaje, desbordando la cola de TCP/IP que normalmente es de 64 KB. Son también afectados por esta técnica casi todos los sistemas basados en Unix y la programación de los routers.

- Land Attack: Consiste en generar un paquete con direcciones IP y puertos de salida y destino idénticos, lo que produce que que el equipo se cuelge al no poder conmutar correctamente los mensajes.

VIII.6 PREVENCIÓN DE LOS VIRUS:

Normas de uso de equipos y soportes:

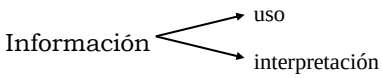
- No bajar archivos de fuentes inseguras.
- Usar de antivirus residentes y actualizados permanentemente.
- Usar de un buen sistema de Back - Up.
- En lo posible no compartir archivos o impresoras.
- No compartir discos, diskettes, cintas o cualquier soporte regrabable con otros usuarios.
- Analizar con antivirus todo e-mail antes de abrirlo.
- Tener siempre diskette o CD de boot para arrancar el equipo en caso de ser afectada esa zona.
- Mantener permanentemente activa la protección contra macrovirus en Word y Excel.
- Enviar copias de archivos en formato RTF en lugar de DOC.
- En caso de recibir spam en su dirección, tramitar inmediatamente el cambio de la misma con el dealer de Internet.
- Usar claves de acceso al equipo y a los protectores de pantalla.
- Utilizar los criterios de cambio de password permanentemente, manteniendo el secreto para todo el personal.-

IX : SEGURIDAD SEGÚN MODALIDAD OPERATIVA

IX SEGURIDAD EN REDES Y COMUNICACIONES:

IX.1 PROBLEMAS:

- Se comparte la información.
- No hay gestión ni control centralizado en cuanto al uso de esa información.



Peligros:

- robo
- alteración
- distribución no autorizada

- Seguridad física, ya que lo que se encuentra distribuido no son sólo estaciones de trabajo, sino también estaciones de procesamiento y todos los componentes de la red de comunicaciones.
- Cableado:

Interferencia (redes de alta tensión, ondas de radio, motores eléctricos cercanos)
- Exceso de longitud - (efecto joule).
- Osciladores: existen en plantas eléctricas, generan grandes campos magnéticos inductivos.

- Virus: problema generado por la cantidad de fuentes de entrada y falta de control.

- Formación de usuarios en los criterios de seguridad informática.

IX.2 MODELO OSI (OPEN SYSTEM INTERCONNECTION):

Protocolo que tiene la forma de varias capas a través de las cuales se arma la transmisión en las redes como un conjunto de reglas que gobiernan el formato y el significado de los marcos, paquetes o mensajes.

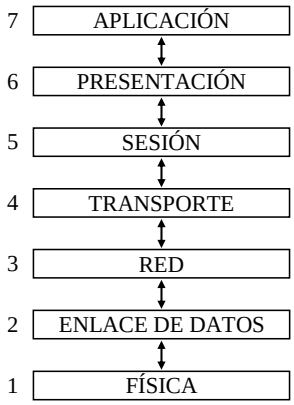
Estos paquetes se intercambian dentro de una misma capa. Estas capas dividen las tareas que componen cualquier comunicación entre computadoras. Estas comunicaciones también pueden ir cifradas y normalmente el cifrado de red se puede realizar de 2 maneras:

- Enlace a enlace:
  Comienza cuando el mensaje sale del enlace físico (equipo donde se genera el mensaje).
  Presenta el inconveniente de hacerse inteligible en muchos puntos ya que todas las cabeceras de destino están cifradas.

- Extremo a extremo:
  Se cifra desde el punto de partida y se descifra en el destino final, ya que las cabeceras no están en la clave y se cifran sólo los datos.

IX.2.1 NIVELES DEL MODELO OSI:

El modelo OSI consta de 7 Niveles:

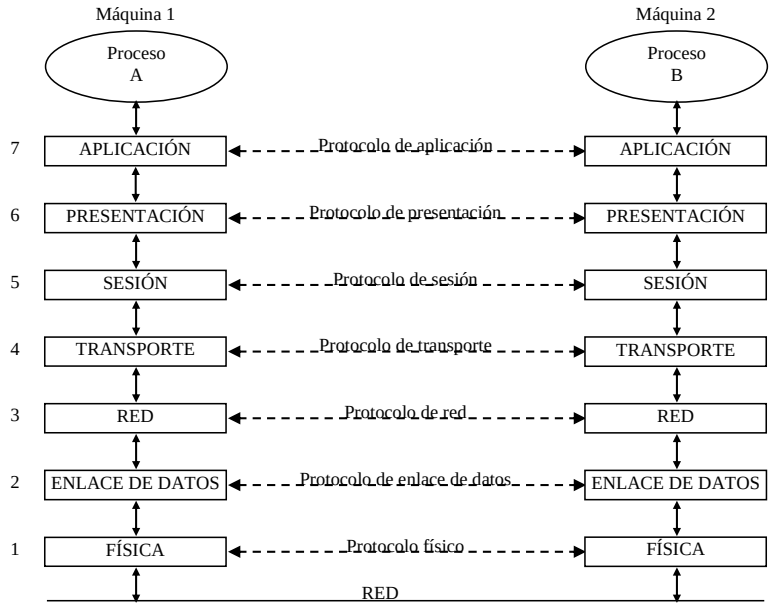


- Relaciones entre los Niveles:

  - Cada nivel desempeña una función bien definida.
  - El objetivo de cada nivel es proporcionar servicios al siguiente nivel superior y proteger al nivel superior de los detalles de cómo se implementan en realidad los servicios.
  - Existe una comunicación virtual (Interfaz) entre dos mismas capas, de manera horizontal.
  - Existe una comunicación vertical (Interfaz) entre una capa de nivel N y la capa de nivel N+1.

Ejemplo:

Cuando el Proceso A de la máquina 1 desea comunicarse con el Proceso de la máquina 2, construye un Mensaje y lo transfiere a la Capa de Aplicación (7) en su máquina. El Software de la Capa de Aplicación añade un ENCABEZADO al frente del Mensaje y lo transfiere a través de la interfaz hacia la capa de Presentación (6). Así sucesivamente cada Capa irá añadiendo su Encabezado y transfiriendo el Mensaje resultante a la Capa inferior. Al llegar al final se transmite el Mensaje. Cuando el Mensaje llega a la máquina 2, se transfiere hacia arriba, y cada Capa lo desmenuza y examina su Encabezado. Por último, el Mensaje queda legible para el Receptor, el Proceso B.



- Funciones:

1 . FÍSICA
Establece las Interfaces a través de señales eléctricas. Puede hacer una transmisión directa de un flujo de bits, manejo de voltajes, etc.
2 . ENLACE DE DATOS
Estructura los datos en un paquete agregando una secuencia especial de bits al principio y al final de cada uno y utiliza una suma de verificación para asegurar su correcta transmisión.
3 . RED
Se encarga del encaminamiento y conmutación de paquetes, de control de tráfico y congestión de la red. Utiliza 2 protocolos: • **X**.25: (Orientado hacia las conexiones): Envía una solicitud de llamada a un destino, el cual puede rechazar la conexión propuesta. Si la acepta el Emisor recibe un ID de Conexión para usarlo en solicitudes posteriores (que utilizan la misma ruta). • IP (Protocolo Internet): Donde no hace falta una comunicación previa. Cada Paquete tiene una ruta hacia su destino independiente de las demás.
4 . TRANSPORTE
Asegura que los paquetes se entreguen sin errores, secuencialmente y sin pérdidas o duplicaciones a pesar de los fallos que pudieran ocurrir en los niveles anteriores. Recibe los Mensajes de la Capa de Sesión y lo divide en paquetes numerados secuencialmente de manera que puede construir la conexión por arriba del X.25 (llegan ordenados) o del IP (como utilizan distintas conexiones pueden llegar desordenados). • Proporciona control de flujo y control de errores.
5 . SESIÓN
Dice cómo se va a utilizar el sistema en las distintas máquinas mediante el uso de primitivas de comunicación. Por ejemplo qué login utilizar entre 2 máquinas. • Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex - full duplex) y su seguridad (contraseñas, etc.). • Función de Sincronización: permite a los Usuarios que inserten puntos de control o verificación en las transferencias de gran tamaño, de modo que si ocurre una falla sólo es necesario llegar al último punto de verificación.
6 . PRESENTACIÓN
Traduce la información del formato de la máquina a un formato

entendible por los usuarios: • Estructura los bits (por ejemplo define los campos de un registro) estableciendo una Sintaxis y Semántica de la información que se transmite. • Define el código a usar para representar cada cadena de caracteres (ASCII, EBCD, etc.). • Administra la compresión de los datos para reducir la información que se transmite. • Define el sistema criptográfico a utilizar.
7 . APLICACIÓN
Se encarga del intercambio de información entre los usuarios y el SO. Es una colección de varios Protocolos para actividades comunes: • Transferencia de Archivos (ftp). • Login remoto (rlogin, telnet). • Correo electrónico (mail). • Etc.

IX.2.2 CONDICIONES DE SEGURIDAD:

- CONFIDENCIALIDAD: requiere que la información sea accesible únicamente por las entidades autorizadas.
- AUTENTICACIÓN: requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa.
- INTEGRIDAD: requiere que la información sólo pueda ser modificada por las entidades autorizadas.
- NO REPUDIO: no permite que un usuario niegue haber recibido un mensaje.
- CONTROL DE ACCESO: donde todo lo que se acceda esté limitado al nivel de autorización del receptor.
- DISPONIBILIDAD: todos los mensajes disponibles en el momento necesario y en el tiempo correcto.

IX.3 LA SEGURIDAD EN WINDOWS NT:

La seguridad en Windows NT es una combinación de técnicas que aseguran un nivel de protección consistente contra los accesos no deseados.

NT gestiona tanto a usuarios como máquinas y sus recursos, debe validar la autentificación de los usuarios y proveerlos de los recursos necesarios para acceder al sistema.

La herramienta básica para administrar los usuarios y grupos de un dominio es el programa USRMGR.EXE, conocido por Administrador de Usuarios para dominios.

Es una combinación de técnicas que aseguran un nivel de protección consistente contra los accesos no deseados. Para implementar la seguridad, tendremos que proteger la red, el sistema operativo y los datos. Para eso, disponemos de la autentificación de acceso propia de Windows NT, seguridad a nivel de objeto y derechos de usuarios, proceso a cargo del administrador del sistema. Para sacar provecho de los más altos niveles de seguridad que permite Windows NT, el nivel de seguridad C2, necesitaremos tanto el hardware como el software adecuados.

NT dispone de herramientas de auditoría que nos permitirán conocer nuestros niveles de seguridad, pero hay que tener muy presentes los temas relativos a la seguridad cuando entran en juego las comunicaciones sobre la Internet. Para estar seguro que estamos protegidos en todos los frentes, es necesario conocer determinadas técnicas.

La seguridad puede ser clasificada en tres diferentes áreas funcionales: seguridad:

- a nivel de red

- seguridad del sistema operativo

- inscripción de datos.

IX.3.1 LA SEGURIDAD DE RED:

Ofrece autentificación (verificando que el servidor de datos y que el receptor de los mismos son correctos) y verificando la integridad de la información (de forma que los datos enviados y los recibidos sean los mismos). Conseguir este nivel de seguridad a nivel de red significa haber implementado un protocolo de red, como TCP/IP, ajustado a las necesidades de la red.

Tras haber definido e instalado una determinada infraestructura de red, añadir y extender protocolos de seguridad es algo teóricamente muy simple.

IX.3.2 LA SEGURIDAD A NIVEL DE SISTEMA OPERATIVO:

De por si debe tener ya un mínimo nivel de seguridad. Si esas funciones básicas de seguridad no han sido implementadas al propio sistema operativo desde un principio, implementarlas con posterioridad será casi imposible. Por ejemplo, Microsoft no fue capaz de implementar una seguridad seria a sus versiones de 16 bits de Windows tras su fase de desarrollo. Fue necesario un nuevo sistema operativo de 32 bits, y un nuevo modelo de programación (la API Win32) para poder hacerlo. Windows NT dispone de unas robustas funciones de seguridad que controla el acceso de los usuarios a los objetos como archivos, directorios, registro de sistema e impresoras.

También incluye un sistema de auditoría que permite a los administradores rastrear los accesos a los archivos u a otros objetos, reintento de inicio de sesión, apagados y encendidos del sistema, etc... En cambio, Windows 95 dispone únicamente de un rudimentario sistema de seguridad en el inicio de sesión, y no dispone de seguridad a nivel de objetos.

IX.3.3 ASPECTOS DE LA SEGURIDAD NT:

NT ofrece seguridad en tres áreas fundamentales. Se trata de *autentificación en el inicio de sesión, seguridad a nivel de objetos y derechos de los usuarios.*

La "Local Security Authority" efectúa validaciones interactivas y remotas, inicios de sesión locales y globales (en dominios) verificándolo contra SAM (Security Account Manager), la base de datos donde se almacenan los nombres de los usuarios y sus contraseñas. La "Local Security Authority" también gestiona los mensajes de auditoría.

El "Security Reference Monitor" verifica si un usuario tiene derecho a acceder a un objeto y ejecutar la acción solicitada. Además, es el responsable de los mensajes de auditoría. Con el diálogo permisos del Administrador de archivos (si se encuentra en NT 3.51) o el Explorador de archivos (en Windows NT 4.0), podrá controlar la seguridad de la mayoría de los objetos. Por ejemplo, la activación y el acceso al objeto servidor del DCOM (en Windows NT 4.0) están completamente integrados con el modelo de seguridad de Windows NT.

Aparte de la seguridad de los objetos, el *NT permite controlar, y monitorizar funciones de sistema.* Con el Administrador de

usuarios podrá controlar qué cuenta de usuario o grupo puede, por ejemplo, añadir estaciones de trabajo a un dominio, salvar o restaurar archivos y directorios, cambiar la hora del sistema, iniciar una sesión localmente, gestionar las registros de auditoría y seguridad y cerrar el sistema.

IX.3.4 ADMINISTRACIÓN DE CUENTAS: AUTENTIFICACIÓN DE INICIO DE SESIÓN:

A un nivel general, un dominio NT es una colección de máquinas, a las cuales el controlador de dominio administra como si se tratase de una única máquina, compartiendo una misma base de datos de seguridad. Dicha base de datos mantiene información de todos los usuarios y grupos de ese dominio. Una cuenta de dominio, llamado de otra forma cuenta global, tiene el formato dominio\usuario. Si iniciamos una sesión en una máquina del dominio e intentamos conectarnos a una unidad de red, tendremos que introducir nuestros datos con ese formato.

Las cuentas de usuarios o grupos en esas máquinas locales tiene el formato **maquina\usuario** y serán exclusivas de esa máquina.

IX.3.5 RELACIÓN CON INTERNET:

A diferencia del bien definido sistema de seguridad del NT, el modelo de seguridad de Microsoft respecto a Internet se encuentra sometido al continuo proceso de cambio al que a su vez se encuentra la misma Internet. El ISF (Internet Security Framework) es hoy por hoy más un compendio de protocolos que una definición de normas de seguridad.

ISF ofrece diversos protocolos de red especializados sobre el estándar de criptografía CAPI de Microsoft y sobre lo que Microsoft denomina Authenticode, un sistema de verificación por firma de objetos instalables, que garantizan que estos módulos u objetos no han sido manipulados y que tienen un autor determinado que de alguna forma,responde de la actuación de dicho objeto software. Los protocolos IFS incluyen:

• PPTP (Point to Point Tunneling Protocol), el cual permite establecer redes seguras sobre segmentos de redes inseguras, creando líneas seguras virtuales.

• SSL (Secure Sockets Layer) y su versión ampliada PTC (Private Communications Technology) que ofrecen autentificación de servidores, encriptación e integridad de datos.

• SET (Secure Electronic Transaction) que permite autentificación y confidencialidad de tarjetas de crédito, vendedores y clientes. SET dispone de un amplio soporte por parte de la industria (Microsoft, IBM, Netscape, etc...) y las últimas especificaciones están disponibles en los sitios web de VISA (http://www.visa.com) y Mastercard (http://www.mastercard.com)

• PFX (Personal Information Exchange) que transfiere información personal entre ordenadores y plataformas.

ISF encripta todos los paquetes de la red. De todas maneras, las aplicaciones pueden disponer de funciones de encriptación adicionales. Por ejemplo, con el código que Microsoft ha licenciado de Nortel (antes Northern Telecomm) y de RSA, Microsoft Exchange puede proteger el correo electrónico con firma/encriptación. La versión estadounidense de MS Exchange también puede utilizar encriptaciones de 56 bits o hasta encriptaciones de 64 bits. Otras versiones, como la española, únicamente pueden utilizar encriptación de 40 bits.

IV IX.3.6 CONSIDERACIONES GENERALES DE SEGURIDAD:

No conviene que NT esté instalado en una máquina con arranque dual, ya que esto haría que muchas de sus garantías de seguridad perdieran efectividad.

Es casi obligado que la partición del sistema sea NTFS. No hay ningún motivo por el que NT haya de instalarse en una partición FAT.

Conviene dar a cada uno de los usuarios del sistema unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esté explícitamente permitido, está prohibido" y continuar explicando todo lo que está permitido. Si se dejan las cosas claras desde un principio, nos ahorraremos muchos quebraderos de cabeza.

Administrador no hay más que uno. Aunque NT permite que haya varios administradores para tareas determinadas, es muy importante delimitar estas tareas al máximo.-

X : CONTINGENCIAS: PREVENCIÓN Y RECUPERACIÓN

X.1 PLAN DE CONTINGENCIAS:

Un plan de contingencia o plan de recuperación en caso de desastre es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace qué y cómo los objetivos de dicho plan son los de restablecer, lo más pronto para la recuperación para posteriormente restaurar totalmente el procesamiento "normal". Un plan de contingencia no duplica un entorno comercial normal (en forma inmediata), pero sí miniminiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.

Dicho de otra manera, un plan de contingencia es un programa de recuperación de la organización. La base de este plan es una decisión del negocio sobre qué aplicaciones de procesamiento de datos son las más importantes de proteger y recuperar. En otras palabras, el plan de contingencia no es sólo un problema del área de sistemas, sino de todo el negocio.

Algunas entidades en las que se desarrolla el esfuerzo de la planeación de contingencia son:

- Aseguradoras.
- Recursos Humanos Corporativos.
- Administración del edificio y de los Servicios.
- Proveedores de Bienes y Servicios de DRP.
- Servicios de Emergencia Locales y Nacionales.

Un plan de contingencia es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de computación. En este plan se define qué tareas son críticas, quién es el responsable de todos los aspectos del proceso de recuperación, y cómo va a funcionar la organización mientras los sistemas están siendo reparados o transportados a un nuevo local.

La pérdida del poder de cómputo puede ser causada por muchas causas, la probabilidad de que ocurran tales eventos puede ser fuertemente reducida a través de un efectivo programa de seguridad. De cualquier forma ya que no puede lograrse la seguridad total, es muy importante tener la capacidad de recuperarse de una contingencia.

X.1.1 UTILIDAD DEL PLAN DE CONTINGENCIAS:

Un plan de contingencia completo mitigará los efectos de esos desafortunados desastres y permitirá una respuesta rápida, una transferencia del procesamiento crítico a otras instalaciones y una eventual recuperación.

La preparación de un plan de contingencia da a los directivos de una empresa una excelente oportunidad para aliviar o minimizar problemas potenciales que, en un momento dado, podrían interrumpir el procesamiento de datos.

Si durante la preparación de un plan de contingencia se identifican y documentan las funciones criticas, se desarrolla un método "formal" de respuesta a las emergencias, y se lleva a cabo procedimientos de respaldo y recuperación, la continuidad y el bienestar del procesamiento de datos en el futuro mejorarán.

Los planes de contingencia son semejantes a cualquier otro plan de negocios: deben tener sentido, ser legibles e indicar todos los aspectos de la función en cuestión. El nivel de detalle para el plan de contingencia, para respaldar la información y para los procedimientos de recuperación, dependen de la importancia de la aplicación y del tipo de información.

Los planes de contingencia han sido desarrollados para los grandes centros de información, así que quizá estos planes y sus metodologías no cubran las necesidades específicas de empresas medianas o pequeñas; por eso, hay que desarrollar un plan de contingencia propio para cada empresa, basándose en la metodología adecuada.

X.1.2 NECESIDAD LEGAL:

Hay tres situaciones donde la planeación de contingencia y la capacidad de recuperación de desastres son legalmente requeridas:
La primera es cuando una ley, estatuto o reglamento requiere que un negocio tenga la capacidad.

La segunda situación es cuando un contrato requiere que el negocio tenga esa capacidad. Bancos, compañías de seguros, y otros negocios grandes ya conocen, en su mayoría, la importancia de la planeación de recuperación de desastres
.
La tercera es lo que los abogados llaman la “ley común”, la cual es contenida en las decisiones de los juzgados y que puede exigir a algunos negocios tener esa capacidad.

X.1.3 ELEMENTOS:

En su concepción, el plan de contingencia es un control netamente preventivo ya que se configura como un instrumento que permite prevención del ambiente informático: tornándose en un control correctivo en la medida en la cual se materializa una contingencia, ya que pretende reducir el impacto de esta.

El diseño e implementación de un plan de esta naturaleza debe contemplar:

- Los riesgos y los porcentajes de factibilidad de éstos, a los que está expuesta la organización.
- La asignación de responsabilidades al personal, tanto en las actividades que realizarán durante la emergencia como en las de preparación y las de recuperación.
- La identificación de las aplicaciones (sistemas automatizados) de mayor importancia dentro de la producción de datos, para darles la seguridad necesaria.
- La especificación de alternativas de respaldo.
- La definición de procedimientos y políticas a seguir durante el momento de la crisis.

La integración de prácticas de mantenimiento entrenamiento en el plan y pruebas del mismo.

Es importante destacar que un plan de contingencia no evita los desastres, sino que provee los medios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así las pérdidas que resultan de estos desastres.

Una de las claves en el desarrollo de n plan de contingencia estriba en la evaluación de posibles riesgos, que envuelven el ambiente informático.

X.1.4 QUIÉN DEBE ESCRIBIR EL PLAN:

A primera vista, contratar a un *consultor externo* con muchos años de experiencia en el desarrollo de este tipo de proyectos puede parecer la mejor opción. Algunas de las ventajas son:

- El desarrollo del plan de contingencia es tan complicado como el de cualquier sistema importante. Por esto, se requiere de una persona dedicada exclusivamente al desarrollo de este proyecto.

- Los consultores poseen conocimientos especializados que pueden facilitar el desarrollo más rápido de un buen plan. Un consultor con experiencia sabe cómo se hace un plan de contingencia y además sabe quién es quién dentro de la industria de seguridad de la información.

- Los consultores, al ser externos a la empresa, miran con un ojo nuevo al proyecto y se percatan de requerimientos que podrían ser pasados por alto por una persona de la empresa.

- Los planes hechos por consultores, típicamente vienen acompañados de un acuerdo de mantenimiento.

Por su parte, la mayor desventaja de contratar a un consultor especializado en el desarrollo de planes de contingencia es su precio: es muy caro, por lo que muchas empresas no estarían en condiciones de pagarlo.

Por otro lado si se decide que el plan sea desarrollado en casa, se tiene las siguientes ventajas:

- El desarrollador del plan de contingencia, al formar parte de la empresa, tendrá un acceso más rápido y completo a la información que necesite.

- El desarrollador del plan, como miembro del área de sistemas, tendrá más facilidad para la realización del inventario de hardware, así como para la etapa de clasificación de los sistemas de acuerdo a su importancia y consecuentemente para la definición de los procedimientos de respaldo.

- Podrá conocer todas las medidas de seguridad de información implementadas en la empresa sin ningunas reservas.

- Puede utilizar el conocimiento que tiene acerca de sus compañeros de trabajo, para tratar de definir quiénes son las personas más adecuadas para la conformación de los diversos equipos de contingencia.

Por lo que respecto a las desventajas de que el plan sea desarrollado por un *empleado de la empresa*, podemos mencionar las siguientes:

- La persona encargada, en la mayoría de los casos no contará con la experiencia necesaria en el desarrollo de este tipo de proyectos.
- Nuevamente en la mayoría de los casos, a la persona encargada de desarrollar el plan se le asignará esta tarea como una adicional a las que ya venía realizando. Es decir, no contará con el tiempo completo para dedicarlo a este proyecto.

X.1.5 RESISTENCIA AL DESARROLLO DEL PLAN DE CONTINGENCIA:

Algunos de los problemas a los que se pueden enfrentar los directivos de Sistemas para obtener el apoyo de la alta dirección para este tipo de proyectos son los siguientes:

a) Falta de justificación de los costos del plan. Esta Crítica puede deberse a que no se justificaron adecuadamente los riesgos de no tener el plan.

b) Si ya contratamos seguros, ¿para qué necesitamos el plan?. Aún si existe consenso para desarrollar un plan en papel, es posible que la gerencia se resista a gastar dinero en su implementación. En forma de responder a la pregunta anteriormente formulada en hacerles entender que los seguros pueden cubrir el costo del daño a la instalación, al hardware y a los medios de almacenamiento de la información. Incluso, los aseguradores pueden ofrecer seguros para la información misma, pero esto no sirve de mucho: un montón de billetes no constituyen la información que necesitamos.

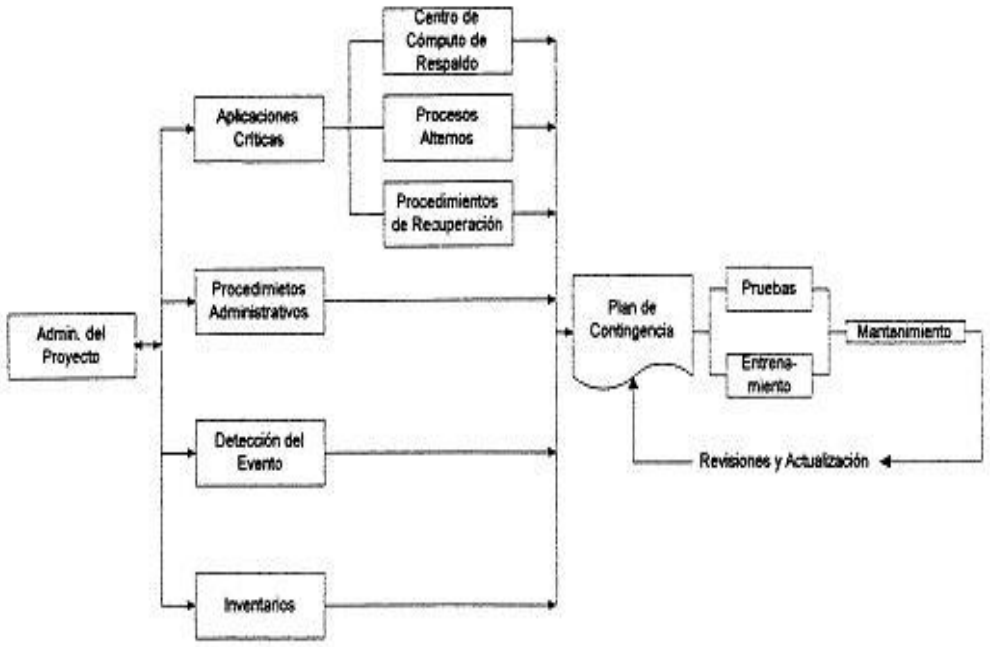
También se debe explicar a la dirección que éste es un proyecto que ahorra dinero. Hay que lograr que la Dirección tenga en mente varias cosas como costo de oportunidad, imagen corporativa, competencia e imagen del negocio. También hay que tomar en cuenta los diversos impactos de la contingencia como el económico, operacional legal, la baja en el servicio, la pérdida del negocio, etc.

X.1.6 CONCEPTOS RELACIONADOS CON LA RECUPERACIÓN DE DESASTRES:

Para entender los aspectos relacionados con la recuperación de desastres y desarrollar mecanismos para poder sobrevivir a las contingencias los coordinadores de planes de contingencia deben investigar la experiencia de otras empresas que han puesto en práctica sus planes.

Una parte importante de la investigación implica la realización de entrevistas con las personas que guiarán equipos de recuperación de desastres en empresas. La investigación incluye también entrevistarse con autoridades de la ciudad y representantes de compañías como las de luz o teléfono, así como con oficinas de manejo de desastres y protección civil del gobierno.

X.2 METODOLOGÍA DE HEWLETT - PACKARD:



Esta metodología consta de 11 etapas. De cada una de ellas se enuncian las principales tareas que la componen.

1. ADMINISTRACIÓN DE PROYECTOS:
   a) Obtener un compromiso preliminar de la Gerencia: la dirección de la empresa debe comprometerse a desarrollar el plan de contingencia en caso de desastre, de tal manera que los recursos necesarios puedan ser asignados al proyecto. Esto implica la distribución de fondos y personal, incluyendo personal del procesamiento.
   b) Organizar el equipo de desarrollo del plan de contingencia: identificar a los individuos de la administración, del procesamiento de datos y usuarios, para que participen en la preparación del programa de recuperación.
   c) Auditar el estado de la preparación del plan de contingencia previo (si existe). Algunos procedimientos e información necesarios para el plan de recuperación de desastres posiblemente ya se han desarrollado y puesto en práctica. Por esto, es importante determinar el estado actual de la preparación. Sabiendo lo que ya existe y lo que falta por hacer, será posible tomar decisiones más realistas sobre el tiempo y los recursos que deben asignarse al proyecto.
   d) Desarrollar un plan administrativo para el proyecto: realizar una estimación de la duración de las tareas, asignar recursos y desarrollar un calendario para el proyecto.
   e) Seleccionar las herramientas de documentación: decidir que paquete o paquetes se usarán para la documentación del plan de contingencia y los procedimientos generales; por ejemplo, quién será responsable de la documentación cuándo se hará, ¿existen normas de la empresa para la generación de este tipo de documentos?, etc.

2. APLICACIONES CRÍTICAS:
   a) Establecer prioridades de las aplicaciones: analizar todas las aplicaciones para priorizarlas e identificar cuáles son críticas. Esta metodología maneja tres categorías: crítica, importante y "todas las demás". Considera que la prioridad de una aplicación se basa en tres factores principales: valor monetario (cantidad de ingresos producidos por la aplicación), limitaciones y prioridades (las aplicaciones pueden ser necesarias por las limitaciones por ejemplo leyes, regulaciones, contratos) urgencia de tiempo (la necesidad de ejecutar una aplicación en periodos o frecuencia determinadas).
   b) Especificar prioridades de procesamiento para la recuperación de desastres: listar las aplicaciones en orden de restauración durante la recuperación. Esta lista sirve para distintos propósito. En primer

lugar, es una herramienta excelente para comunicar las prioridades de procesamiento que serán seguidas en caso de desastre. En segundo lugar, es utilizada en las siguiente actividad, en donde se deben determinar los requerimientos de procesamiento para cada tipo de prioridad. Esto, a su vez, se usa para establecer los objetivos de recuperación y para seleccionar las instalaciones de respaldo apropiadas. Finalmente, es un paso preliminar en el desarrollo de un plan de restauración.

c) Determinar los requerimientos del procesamiento: analizar los recursos necesarios para procesar las aplicaciones con prioridad alta, de tal manera que se tanga suficiente capacidad de respaldo. Una decisión clave que debe tomarse es definir cuántos niveles de prioridad van a ser respaldados.

d) Establecer objetivos de la recuperación de desastres: especificar el nivel de procesamiento y tiempos de recuperación que se han de lograr en la restauración de desastres menores, mayores y catastróficos.

3. INSTALACIÓN DE RESPALDOS Y PROCEDIMIENTOS:

a) Seleccionar una localidad externa de almacenamiento (caja de Seguridad): los datos y documentación de respaldo deben almacenarse fuera de la instalación de respaldo para que sobrevivan, aun cuando exista una destrucción total del centro de cómputo. En esta etapa se deben identificar una o más localidades externas donde se puedan almacenar seguramente los datos y documentación de respaldo.

b) Determinar el contenido indispensable de la caja de seguridad externa: identificar los archivos, programas, documentación, materiales, etc., específicos que deban ser respaldados y mantenidos en un lugar fuera de la instalación.

c) Especificar procedimientos de almacenamiento y actualización: determinar los procedimientos, calendarios y responsabilidades de mantenimiento del contenido de la caja de seguridad externa. Se necesitan políticas y procedimientos para asegurar la actualización adecuada de estos materiales, ya que en caso de que un desastre destruya la instalación primaria junto con su contenido, únicamente el respaldo mantendrá en operación a la compañía.

d) Identificar los requerimientos del sistema para las instalaciones de respaldo: determinar el equipo y la capacidad de procesamiento necesaria en la instalación de respaldo. El propósito de esta tarea es investigar qué recursos de cómputo son necesarios en la instalación de respaldo: tiempo, sistemas, periféricos, comunicaciones de datos

y otros equipos, para procesar las aplicaciones de determinada prioridad.

e) Seleccionar una o más de estas instalaciones: evaluar las instalaciones potenciales de respaldo y elegir una o más para hacer los arreglos necesarios. El plan de contingencia en caso de desastre debe tomar en cuenta un rango de posibilidades desde un desastre menor, tal como una suspensión de cómputo prolongada, hasta un desastre catastrófico que destruya totalmente el centro de cómputo.

f) Producir una guía de respaldo de la instalación: una o más instalaciones de respaldo han sido seleccionadas para ser usadas durante la recuperación de desastres. Estas instalaciones se diferenciarán entre si y del centro de computo primario. La información especifica de cada una debe documentarse en una guía de la instalación de respaldo.

g) Identificar al personal de respaldo: idealmente, el personal del centro de cómputo estará disponible durante un desastre de cualquier modo, si no está disponible, entonces sus funciones tendrán que ser realizadas por otras personas (el personal de respaldo).

4. PROCEDIMIENTOS DEL PROCESAMIENTO ALTERNO:

a) Identificar las aplicaciones críticas que requieren procedimientos del procesamiento alterno: las aplicaciones críticas son, por definición, aquellas necesarias para la supervivencia de la compañía; el plan de contingencia, en caso de desastre, proporciona restauración para estas aplicaciones. Es necesario considerar la posibilidad de que la recuperación toma tiempo, dependiendo del tipo de desastre y de las alternativas de respaldo que hayan sido seleccionadas. Por esto, puede ser necesario desarrollar procedimientos para que el procesamiento alterno de estas aplicaciones puede continuar, incluso antes de que el procesamiento de cómputo se haya restablecido. Se debe considerar cuidadosamente la decisión de crear procedimientos alternos. Un procedimiento alterno no siempre puede ser viable o necesario para cada aplicación crítica.

b) Desarrollar los procedimientos de procesamiento alterno: para las aplicaciones criticas seleccionadas, se debe crear el procedimiento de procesamiento alterno, que pueda usarse en caso de que las instalaciones del centro de cómputo no estén disponibles. Con una gran disponibilidad de computadoras personales, se pueden desarrollar procedimientos alternos basados en PC.

5. PROCEDIMIENTOS DE RECUPERACIÓN:

a) Definir equipos de recuperación y sus funciones: las acciones que se deben tomar para efectuar el restablecimiento de un desastre, son

llevadas a cabo por equipos de recuperación, cada uno con su propia área de responsabilidad. El propósito de esta tarea es especificar los equipos de recuperación y las funciones de cada uno.

b) Identificar a los miembros de cada equipo: nombrar a las personas que servirán en cada equipo de recuperación.

c) Especificar sus procedimientos: establecer los pasos de acción que tiene que seguir los lideres y miembros del equipo. Se debe distinguir entre lo que debe realizar el líder y lo que pueden hacer los otros miembros.

6. PROCEDIMIENTOS DE DETECCIÓN DE EVENTOS:

a) Especificar los procedimientos de emergencia: los procedimientos de emergencia son las acciones que deben realizarse inmediatamente, en respuesta a un evento dañino o a una situación amenazadora.

b) Establecer los procedimientos de escalación: el propósito de estos procedimientos es definir la distribución de los pasos y del tiempo que llevan a la declaración de un desastre menor.

7. PROCEDIMIENTOS DEL EQUIPO DE MANEJO DE DESASTRES (EMD):

a) Identificar a los miembros del equipo de manejo de desastres: este equipo tiene la responsabilidad de dirigir las operaciones de recuperación y la restauración de procesamiento normal. En esta tarea se debe seleccionar al Gerente de Recuperación de Desastres, al Coordinador del Equipo de Recuperación y a los Líderes de los Equipos.

b) Especificar las funciones y los procedimientos del equipo: el Equipo de Manejo de Desastres está orientado a los esfuerzos de recuperación que siguen al desastre. Para asegurar que el equipo pueda funcionar efectiva y eficientemente, su responsabilidades son establecidas en el estatuto formalizado junto con sus funciones en caso de desastre. Además, los pasos de acción necesarios para iniciar las operaciones de recuperación deben estar claramente indicados en forma de procedimientos y listas de verificación.

c) Seleccionar las ubicaciones de los centros de control: elegir localidades internas y externas para usarse como centros de control. Las operaciones de desastres se deben dirigir desde este y su propósito puede establecerse en una sola palabra: comunicación. Proporciona administración y control coordinado de todas las comunicaciones durante la recuperación de desastres. Cuando se declara un desastre y durante las operaciones subsecuentes de reestablecimiento, todos los equipos y el personal estarán en contacto continuo con el centro de control. Por esto, es importante

que todos sepan dónde estará el "centro nervioso" durante una emergencia.

d) Listar los recursos del centro de control: el centro de control debe estar bien equipado, especialmente con herramientas de comunicaciones. Las comunicaciones son altamente críticas cuando el rescate y la atención médica son las necesidades primarias, y el tiempo es esencial; particularmente cuando la familia del personal clave se encuentran en peligro. Una lista de verificación de los recursos y registros necesarios en el centro de control activado minimizará el tiempo necesario para hacerlo funcionar.

e) Realizar un inventario del material necesario para las aplicaciones críticas: la evaluación del daño del impacto son actividades clave de la administración de desastres porque proporcionan la información necesaria para la toma de decisiones. A fin de elegir una alternativa de recuperación, la administración debe tener respuesta a dos preguntas básicas: 1) ¿qué se ha dañado o perdido? 2) ¿en qué forma han sido afectadas las aplicaciones críticas por el daño o la pérdida?. Un inventario completo y categorizado puede servir como base para la evaluación del daño del impacto.

8. INVENTARIO (LO QUE SE TRATA DE PROTEGER):

a) Llevar un inventario de todos los recursos del procesamiento de datos: el inventario debe dividirse en categorías y después subdividirse dentro de esas categorías, para hacer más fácil la recopilación, la actualización y el uso. Se deben recopilar listas de hardware, software, equipos, materiales y otros recursos usados para el procesamiento de datos.

b) Listar a los distribuidores de los recursos críticos: las partidas dañadas en un desastre pueden tener que ser reemplazadas rápidamente, especialmente aquellas usadas por aplicaciones críticas. Para obtenerlas lo más fácil y rápidamente posible, es necesario recopilar información de distribuidores, por lo menos de cosas utilizables en el procesamiento de aplicaciones con prioridad alta.

9. ENTRENAMIENTO:

a) Diseñar un plan completo para el entrenamiento de recuperación de desastres: es necesario un programa general de entrenamiento para asegurar que las personas correctas obtengan el tipo de adiestramiento adecuado. A pesar de que muchas personas necesitan un entrenamiento, no todos requieren el mismo. Es decir, debe entrenarse a cada persona en las funciones que tiene asignadas en el plan de contingencia, esto es, en las funciones que desempeñará el equipo o equipos de recuperación al que pertenezca.

El programa debe llevarse lo más simplemente posible, al determinar las diversas necesidades de capacitación. Por lo menos debe incluir objetivos, programas, calendario y clasificación.

b) Desarrollar actividades específicas de entrenamiento: el plan de instrucciones de cada una de las actividades en el programa de adiestramiento debe seguir cualquier formato acostumbrado o conveniente. Lo esencial es hacer que los planes sean específicos, claros y completos. Los objetivos deben ser específicos y describir lo que los estudiantes podrán hacer como resultado del adiestramiento.

c) Desarrollar técnicas y herramientas de evaluación: el entrenamiento tiene como función primaria el desarrollo de conocimiento y la habilidad. También es una buena fuente de información sobre la calidad del plan de contingencia en caso de desastre. Durante el curso de adiestramiento, ciertas secciones pueden no estar claras o tal vez no sean funcionales. Es por eso que las técnicas de evaluación deben dirigirse para contestar tres preguntas básicas: 1) ¿son capaces los estudiantes de llevar a cabo sus responsabilidades de recuperación? 2) ¿cómo puede mejorarse el entrenamiento? 3) ¿cómo puede mejorarse el plan de contingencias?

10. PRUEBAS:

a) Diseñar un programa completo del plan de contingencias: las pruebas del plan de contingencias deben llevarse a cabo de manera cuidadosa y sistemática. Los puntos claves que deben incluirse en este programa son: objetivos, políticas y guías, responsabilidad gerencial de las pruebas, especificación de las pruebas.

b) Desarrollar planes para pruebas específicas: escribir un plan para cada prueba que debe ser conducida.

c) Desarrollar técnicas y herramientas de evaluación de las pruebas: las pruebas del plan de contingencia proporcionan información importante sobre la adecuación del plan y de entrenamiento. Por ello, esta tarea está dedicada a las técnicas y herramientas que usarán para reunir esta información.

11. MANTENIMIENTO:

a) Asignar responsabilidades para la administración y el mantenimiento del plan de contingencia: el mantenimiento del plan de contingencia involucra varias funciones:

- Recibir y controlar información de las revisiones necesarias.
- Mantener una lista de distribución de las copias del plan y controlar su circulación.
- Mantener la historia de revisiones del plan.

- Asegurar que las revisiones se llevan a cabo puntualmente
- Distribuir las actualizaciones como sea necesario.
- Coordinar el ciclo de revisión con los calendarios de entrenamiento y de pruebas.
- Coordinar con los auditores el calendario de revisiones y mantenimiento.

b) Establecer procedimientos y calendario de revisión y mantenimiento: los propósitos de esta tarea son proporcionar un calendario para la revisión regular y sistemática del contenido del plan de contingencia en caso de desastre y definir un procedimiento para los cambios sugeridos. También será útil para los centros de reunión de datos a fin de identificar los cambios necesarios.

c) Crear listas de distribución y políticas para el programa de recuperación: el plan de contingencia contiene mucha información sensible sobre las operaciones de cómputo y comerciales de la compañía; por ejemplo, aplicaciones criticas, ubicación de la caja de seguridad externa, arreglos para las instalaciones de respaldo, etc. Es por esto que la distribución del plan de recuperación es un punto que merece una consideración cuidadosa.-

XI: AUDITORÍA DE SISTEMAS – CONCEPTOS GENERALES

XI.1 DEFINICIÓN:

Técnica que evalúa los sistemas de control.

XI.1.1 HISTORIA:

Aparece con la necesidad de controlar a la distancia:

- Oidores reales.
- Auditores de Cuentas.
- Auditores Contables.
- Auditores Operativos.
- Auditores Informáticos.

XI.1.2 TIPOS:

- Auditoría Externa: observa el desenvolvimiento de la entidad en su conjunto. Características:
  - Quién la hace: Puede ser de una entidad supervisora (BCRA, Organismos Internacionales de Crédito) o una consultoría ad-hoc.
  - Quién la planifica: el organismo que la hace en base a sus objetivos.
  - Para qué: Conocer el nivel de seguridad operativo, contable y de información que ofrece el funcionamiento de la empresa y si éste se adecua a las normas prefijadas.
  - Para quién: Siempre para el mayor nivel de la empresa.

- Como opera: Revisión documental, cuestionarios, circularizaciones, comprobación operativa, informes y recomendaciones.

- Auditoría Interna: u Operativa; observa el desenvolvimiento de determinados sectores o parte de los mismos. Características:

  - Quién la hace: Puede ser de una consultora externa o un sector propio de la organización.

  - Quién la planifica: el organismo que la hace en base a sus objetivos.

  - Para qué: Conocer el nivel de seguridad operativo, contable y de información que ofrece el funcionamiento del sector analizado y si éste se compadece con lo pautado por la organización.

  - Para quién: Para el mayor nivel de la empresa o como mínimo para los niveles gerenciales.

  - Como opera: Revisión documental, cuestionarios, circularizaciones, comprobación operativa, comparación con standares propios, informes y recomendaciones.

XI.2 AUDITORÍA DE SISTEMAS DE INFORMACIÓN:

O Auditoría Informática (AI); comprende la Auditoría de todos los sistemas que, parcial o totalmente, utilizan recursos informáticos en su operatoria.

Características:

- Especialización: muy alta en Informática; también en Auditoría Operativa.

- Donde se aplica:

  - Desarrollo de Sistemas: controles, puntos de control, seguridad física y lógica, claves, encriptación, resguardos físicos, pistas de AI, mecanismos de recuperación.

- Sistemas en Producción: seguridad de: Centro de Cómputos, equipos locales y remotos, sistemas de comunicación, sistemas operativos y bibliotecas; mantenimiento; resguardos; uso de claves; políticas de personal; procedimientos formales; segregación de funciones; documentación; controles de E/S; Plan de Contingencia.

➢ En que tipo de Auditoría: en todas.

➢ Tendencia futura: Crecimiento geométrico; incluirá e-comerce.

➢ Principales problemas: Pocos especialistas. Poca bibliografía. Falta de normas. Pocos programas utilitarios (SIAC, ACL). Alta complejidad técnica junto con necesidad de amplia experiencia.

➢ Que busca: la mal función de la información en la empresa, por ejemplo: debilidades en los puntos donde se ubica la información; resultados negativos en los SDI; falta de actualización del personal usuario; poco involucramiento de los usuarios en los SDI; adm. débil o informal de los proyectos; carencia de análisis costo/beneficio en los proyectos; metodologías deficientes o inexistentes; falta de planeamiento; poco involucramiento de la Dirección; proyectos de AI esporádicos o informales.

XI.2.1 REQUISITOS DEL ÁREA Y PERSONAL DE AUDITORÍA:

➢ Área: dependencia y amplio apoyo del máximo nivel; disponibilidad de recursos internos y externos amplios; posibilidad de generar su propia planificación; posibilidad de modificar sus propias normas; autorización de acceso a todo nivel de los recursos informáticos.

➢ Personal: Consustanciado con la función; amplia especialización y constante capacitación; experiencia o conducción por seniors; en equipos combinados (internos y externos) siempre dirección del interno; evaluación por resultados de mejoras, no por detección de errores; capacidad de encontrar errores y recomendar soluciones.

XI.2.2 APLICACIONES DE LA AI:

➢ En organismos oficiales: normalmente buscan el cumplimiento de normativas emanadas de leyes, decretos, resoluciones, etc. que

rigen su actividad. Son muy difíciles de realizar por encontrarse las presiones políticas en todos los pasos (cualquier observación perjudica a un color político, actual o anterior), la resistencia sindical de los gremios (que pierden poder ante sus representados), y la estabilidad de los empleados (que impide tomar medidas ante la ineficiencia).

Los principales organismos de control son:

- A nivel Nacional: Auditoría General de la Nación, tiene injerencia sobre cualquier acto de gobierno que implique los intereses del país. Sindicatura General de Empresas Nacionales (SIGEN), auditan las empresas del Estado Nacional. Oficina Anticorrupción (ex Secretaría de Ética Pública), investiga denuncias de cualquier tipo, aún su función no está bien definida.

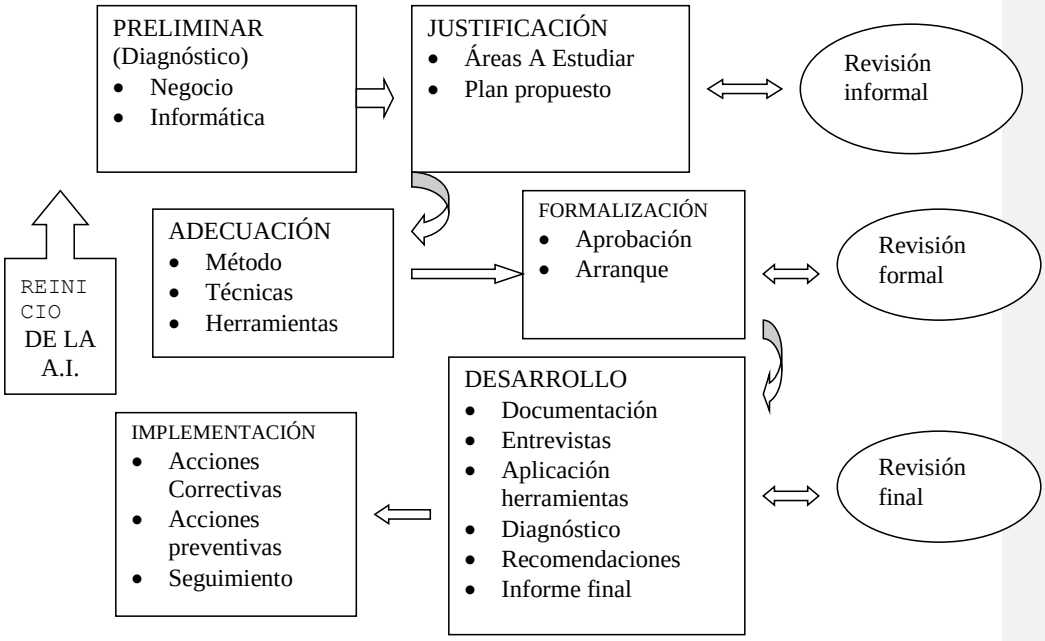
- A nivel Provincial: Tribunal de Cuentas; teóricamente es un organismo independiente que interviene en todos los actos de Gobierno que puedan afectar el patrimonio provincial. En realidad tiene también un alto contenido político y es sometido a presiones por parte de gobernantes y legisladores. Su propia reglamentación, que le da la propiedad de un control ante, durante y después de la acción de Gobierno, le da un carácter burocrático que lo torna ineficiente. En la mayoría de las provincias fue reemplazado por sistemas de Auditoría modernos.

- Empresas Privadas: Para Auditoría Externa suelen contratar consultoras reconocidas a nivel internacional, evitando sobre todo los estudios locales en comunidades pequeñas. Para Auditoría Interna se suele crear un sector interno, dirigido por un senior y conformado por personal nuevo en la empresa, total o parcialmente (cuando se incorpora personal especializado para un trabajo en particular).

- Entidades Financieras: los bancos, financieras, cajas de crédito y compañías de seguros tienen un régimen especial ya que están sometidas a las disposiciones del BCRA; por lo tanto son sometidas a la Auditoría (contable y de Sistemas) del BCRA, a su propia Auditoría Externa, que sólo se contrata con las grandes consultoras especialistas en el tema y Auditoría Interna similar a las empresas privadas, pero con mayor

intervención. La Auditoría del BCRA no sólo se realiza de acuerdo a sus propias normas (2659) sino que califica a la entidad de acuerdo a los resultados, permitiéndole expandir o limitándole sus actividades mediante la calificación CAMEL; también puede requerir informes, documentación y hasta papeles de trabajo de las auditorías externa e interna de la entidad.

XI.2.3 DESCRIPCIÓN DEL CICLO METODOLÓGICO DE LA AI:



- PRELIMINAR O DIAGNÓSTICO: Comprende un conocimiento genérico de la empresa y su relación con la informática. Se basa en una serie de averiguaciones sobre el negocio que, como mínimo, deben contener:

  - Misión del negocio
  - Capital en giro
  - Organigrama general
  - Áreas del negocio
  - Macroproyectos del negocio
  - Objetivos del negocio
  - Políticas referentes a informática
  - Áreas de oportunidad que se derivan de la informática

  V Obtener calificaciones de las soluciones informáticas actuales (basada en 5 niveles):

  - Soluciones aportadas por consultorías externas, en cuanto a estrategias para obtener las soluciones de negocio
  - Nivel de Sistematización de los procesos del negocio, para las funciones operativas tácticas y estratégicas
  - Nivel de desarrollo tecnológico, sobre la tecnología de vanguardia en informática y telecomunicaciones
  - Niveles operativos, instalaciones, capacitación del personal (de Sistemas y usuarios), atención a fallas de soft y hard
  - Aspectos administrativos del área informática (misión, organigrama, proyectos, etc.)

- Aspectos técnicos, soft instalados, aplicativos funcionando, información gerencial existente, hard instalado

- Experiencias anteriores de AI

➢ JUSTIFICACIÓN: Comprende la detección y evaluación de los posibles riesgos a que está expuesta la organización en razón de su dependencia informática. Básicamente se quiere alcanzar una matriz de riesgos (donde se enumeran los mismos y se les da una calificación estimada) por cada área en análisis.

La matriz debe contener columnas que describan lo siguiente:

- Área a analizar, pudiendo ser de Sistemas solamente u otras relacionadas

- Aspectos a evaluar del área, que condiciones se considera que deben entrar en la AI

- Porcentaje de riesgo por aspecto, de manera que el total de 100% para el área

- Porcentaje de riesgo del área en el % total de las áreas a auditar, debe redondear el 100%

- Secuencia sugerida para auditar, en base a los porcentajes requeridos para cada área

Por ej.: supongamos que se quieren auditar solamente las siguientes áreas y la experiencia, el relevamiento de alto nivel y las características de la instalación indican los porcentajes indicados:

Matriz de riesgos para A.I.:

ÁREA	ASPECTOS A EVALUAR	% RIESGO POR ASPECTO	%RIESGO POR ÁREA	SECUENCIA PARA AUDITAR
Gcia.de Sistemas	Planificación estratégica	12	22	3
	Informes de niveles inferiores	3		
	Control de la seguridad	6		
	Supervisión sobre el personal	1		
Jefatura Desarrollo	Planificación táctica	8	14	4
	Supervisión directa de analistas y programadores	1		
	Control de bibliotecas	5		
Jefatura de Mantenimiento	Planificación táctica	2	38	1
	Supervisión directa de analistas y programadores	12		
	Actualización de documentación	15		
	Control de versiones	9		
Procesamiento de Datos	Planificación diaria	5	26	2
	Sistema de back-up	11		
	Control de perfiles	5		
	Control de bibliotecas	3		
	Control de acceso	2		
TOTAL		100	100	

Además se debe elaborar un Plan Propuesto; en base a la matriz de riesgo se logra un plan por PERT, estimando los tiempos en base a la importancia de los porcentajes de la matriz y en los recursos tanto el tiempo de los auditores como del personal usuario que se verá afectado y del personal auxiliar (programadores, especialistas, etc.) que se contraten especialmente para la tarea. Se realizarán reuniones informales con el máximo nivel hasta consensuar un plan satisfactorio.

- ADECUACIÓN: Se debe realizar en base a todos los elementos que requerirá la AI de acuerdo al Plan Propuesto de la fase anterior. Aquí se debe definir por escrito:

  - Objetivos concretos del proyecto
  - Detalle de las tareas a realizar y sus responsables
  - Productos esperados
  - Elementos a auditar por área de revisión
  - Métodos, técnicas y herramientas a utilizar
  - Personal a contratar, calificación, costo y tiempo
  - Políticas y procedimientos que se van a controlar por área
  - Elaboración de cuestionarios a utilizar.

En este punto se debe presentar a la autoridad correspondiente en formato proyecto con un tiempo de respuesta acordado para la respuesta.

- FORMALIZACIÓN: El objetivo de esta fase es justificar el proyecto en base a todos los argumentos encontrados y analizados en las faces anteriores obteniendo la aprobación formal que servirá como respaldo de las futuras acciones. Los puntos a desarrollar son:

  - Verificar prioridades
  - Verificar planificación
  - Presentar formalmente el proyecto
  - Conseguir la aprobación formal del proyecto

  Llegado a este punto, se cuenta con un proyecto aprobado que permite el arranque de las funciones específicas de AI:

  - Presentación del proyecto a los usuarios involucrados

- Concertar visitas, entrevistas, recepción de documentación, etc, según planificación.

- DESARROLLO: En esta fase se realiza la AI propiamente dicha; las técnicas a seguir se describen en otros puntos, pero la secuencia de pasos es la siguiente:

  - Reunión de la documentación y comprobación de la autenticidad de la misma

  - Realización de las entrevistas, personales o por medios indirectos (fax, e-mail, etc.), siempre basadas en un cuestionario previamente descripto; en ellas deben incluirse las inspecciones físicas a los sitios auditados

  - Aplicación de herramientas, fundamentalmente las descriptas para usar con el computador en base a los métodos aplicados

  - Elaboración de un diagnóstico, consensuado con todo el equipo que participó; no debe tener una única calificación o conclusión, sino ser sólo una enumeración de falencias o debilidades que se han encontrado en el transcurso de la AI; se debe hacer conocer a los usuarios con la advertencia que puede no corresponder al informe final, recogiendo y analizando los comentarios de los mismos

  - Elaboración de recomendaciones, una vez depurado el diagnóstico, en una tarea conjunta con todo el equipo de AI se deben elaborar y fundar las recomendaciones que permitirán superar los problemas diagnosticados, teniendo en cuenta el entorno posible

  - Informe, incluye el diagnóstico y, por cada situación diagnosticada como débil o errónea, debe adjuntarse una sugerencia que permita superar el problema; el Informe se entrega a la máxima autoridad de la empresa quien dispone su distribución y eventual aplicación

- IMPLEMENTACIÓN: Se trata de implementar y controlar el uso de las sugerencias aportadas por el Informe de AI; se debe acordar con el máximo nivel y producir Informes Auxiliares o notas relacionadas por cada actividad que se desarrolla:

  - Acciones correctivas, son aquellas que deben implementarse inmediatamente para salvar una situación errónea

- Acciones preventivas, medidas que pueden tomarse en un lapso de tiempo medio (en general 1 o 2 meses) y tienden a asegurar la operatoria informática contra ataques o errores a la que hoy está expuesta

- Seguimiento, determina el mínimo de inspecciones de AI que en el futuro deberán hacerse para asegurar las acciones sugeridas, tanto en tiempo como en recursos.

XI.3 INFORME FINAL:

La función de Auditoría se materializa exclusivamente por escrito, por ello la elaboración final es el exponente de su calidad.

Existen informes en borrador previos que sirven para contrastar opiniones entre auditor y auditado que pueden permitir descubrir fallos en la apreciación del auditor.

La estructura del Informe debe respetar al menos los siguientes aspectos:

- Fecha de comienzo de la Auditoría y fecha de redacción del Informe
- Nombres del equipo auditor y de todas las personas entrevistadas, con indicación de cargo y responsabilidades que cada uno ostenta.
- Definición de objetivos y alcances de la Auditoría
- Ennumeración de los temas considerados, donde por cada uno se expondrá:
  - Situación actual; si la revisión es periódica, se recordará su evolución en el tiempo
  - Tendencias, mediante parámetros que permitan determinarlas
  - Puntos débiles y amenazas, con evaluación de riesgos
  - Recomendaciones y Plan de Acción

El Informe deberá estar precedido por una Carta de Introducción, que debe tener las siguientes características:

- Como máximo de 4 páginas
- Incluirá fecha, naturaleza, objetivos y alcances
- Cuantificará la importancia de las áreas analizadas
- Proporcionará una conclusión general, concretando las áreas de gran debilidad
- Presentará las debilidades en orden de importancia y gravedad
- No incluirá recomendaciones.

En general, la redacción del Informe debe ajustarse a las siguientes pautas:

- El Informe incluirá sólo hechos importantes
- Deberá consolidar con verificación objetiva y pruebas documentales todos los hechos que se describen
- Los hechos analizados deben poder ser sometidos a cambios
- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación actual
- El cambio propuesto debe superar a todas las alternativas viables
- Los hechos mencionados en el Informe deben estar acompañados por las consecuencias, repercusiones y conclusiones que el mismo implique

Las recomendaciones de AI deben entenderse por simple lectura, estando completamente soportadas en el propio texto.-

XII : MÉTODOS DE AUDITORÍA INFORMÁTICA

Básicamente se debe distinguir dos tipos de métodos de AI:

XII.1 ALREDEDOR DEL COMPUTADOR:

Son controles específicos de entorno de las actividades informáticas, sin utilizar directamente el computador. Pueden ser:

- Existencia de métodos de resguardo de información
- Verificación de métodos escritos de recuperación de back-up
- Condiciones de alojamiento físico de los back-up (protección contra fuego, robo, catástrofes, etc.)
- Forma de registro de los back-ups
- Utilización de rótulos externos e internos
- Comprobación de los vencimientos de los back-ups
- Verificación de ensayos periódicos de recuperación
- Existencia de Manuales de Operaciones, incluyendo recuperaciones de procesos abortados y su actualización
- Verificación del conocimiento específico de los operadores de Sistemas
- Organización del área Sistemas, con discriminación de funciones
- Documentación actualizada y completa de programas, sistemas y procedimientos
- Control de versiones de los programas
- Procedimientos de puesta en producción
- Certificación de propiedad de los sistemas
- Existencia de la bitácora del centro de cómputos
- Correcta identificación de los outputs
- Seguridad física externa: restricciones de ingreso; registros de ingreso/egreso; detectores de humo; protección contra incendios; tipo de ambiente (mobiliario, paredes, revestimientos, etc.); aire acondicionado, equipamiento redundante, mantenimiento, regulación, limpieza de ductos, etc.; protección contra asaltos, catástrofes naturales, contaminación (terminales), etc.; instalación y acceso al cableado lógico; protección de las líneas de comunicación; redundancia de las instalaciones; abastecimiento eléctrico (líneas, UPS, grupos electrógenos, protección contra rayos y corrientes residuales); iluminación de emergencia; controles sobre equipos de contingencia
- Métodos para delimitación de acceso (por SO y por aplicativos)
- Constancias de habilitación y uso de passwords
- Autorización para definir perfiles de usuario
- Designación y actuación del Comité de Sistemas y el Responsable de Seguridad

- Constancias de guardado de las claves de Administración de Seguridad
- Existencia de Planes de Contingencia para distintos niveles de acontecimientos
- Existencia de convenios de procesamiento alterno
- Existencia de convenios de mantenimiento
- Contrataciones vigentes con proveedores de hardware y software
- Resguardos físicos para documentación sensible que se reciba en el centro de cómputos
- Verificación de circuitos de recepción y entrega de documentación.

XII.2 USANDO EL COMPUTADOR:

El uso directo del computador amplía sensiblemente las posibilidades de la AI; sin embargo, nunca reemplaza la Auditoría Alrededor del Computador, sino que son complementarias, ya que ésta dará los elementos de juicio para el entorno de funcionamiento y el uso necesario de controles externos al procesamiento. Las principales ventajas que se obtienen al usar el computador para lograr elementos de juicio válidos y suficientes son las siguientes:

- Posibilidad de realizar análisis 100% de los datos, eliminando la incertidumbre de los muestreos.
- Celeridad y seguridad en el procesamiento.
- Rápida separación y cuantificación de los datos que reúnen una característica determinada.
- Posibilidad de seleccionar muestras totalmente al azar sin influencia sistemática.
- Posibilidad de seleccionar items de particular interés del auditor sin intervención de otro personal (TXT).
- Introducir datos de prueba y comparar con resultados esperados.

Los requerimientos para utilizar el computador como centro de la AI tiene algunas restricciones:

- Se debe contar con suficientes pistas de auditoría
- Tener documentación de apoyo idónea
- Poseer información de las salidas adecuadas
- Conseguir medios de totales de control de los archivos durante los procesos
- Obtener muestras de las transacciones interactivas
- Poseer informaciones intermedias durante el procesamiento de los datos.

XII.2.1 VARIANTES DEL USO DEL COMPUTADOR:

Se dan 3 variantes para el uso del computador:

- Paquetes de Auditoría: Programas o sistemas parametrizables por el auditor para casos particulares que se usan en los equipos de producción. Pueden adquirirse por separado o vienen incluidos en los SO (caso OS/400). Dentro de sus funciones pueden estar: lectura de archivos, querys on-line, realización de cálculos, armado de informes especiales, rastreo de datos; en OS/400: cantidad de tentativas rechazadas de ingreso de passwords, errores de acceso, creación, borrado o modificación de objetos, arranque y parada de trabajos, retención, liberación cambios y desconexiones de trabajos, violaciones a la firewall, en los programas: bloqueo de instrucciones, violación de dominio de objetos, restauración de programas que adoptan perfil del usuario; en los perfiles de usuario cambios, creaciones y autorizaciones del de grupo; en herramientas especiales: arranque de herramientas de servicio del sistema, arranque de copia de pantalla. Son caros pero fáciles de usar y la capacitación del auditor permite su uso repetido en distintas instalaciones.

- Programas de Auditoría específicos: Se desarrollan a pedido del auditor para un fin específico. Requieren un esfuerzo de diseño y programación apreciable si se lo compara con su uso limitado a una situación especial. También aumenta el costo de capacitación del auditor para utilizarlo. Se usa en casos muy particulares; en caso que el equipo de AI tenga capacidad para hacerlo, debe extremarse el cuidado en el tratamiento de datos de producción, debiendo trabajar preferiblemente con copias de las bases o archivos a auditar.

- Programas utilitarios específicos: Son programas especialmente desarrollados par el uso en AI por medio de una PC en la que se vuelcan archivos TXT obtenidos de los equipos en producción. Son de alto costo pero de fácil utilización, teniendo además la ventaja de no requerir prácticamente la intervención del área auditada. SIAC y ACL son los más difundidos, por su entorno amigable y la gran cantidad de funciones que permiten, basados en la conversión de los archivos ingresados en bases de datos relacionales y su posibilidad de explotación en base a querys, asociación de claves, etc.

XII.3 METODOLOGÍAS A TRAVÉS DEL COMPUTADOR:

Son formas genéricas de encarar el trabajo usando el computador como herramienta. Se pueden usar aisladas o combinadas.

XII.3.1 MINICOMPAÑIA:

Permite comprobar el funcionamiento de rutinas, programas o aplicaciones parciales, en condiciones normales de producción. Se define como "una modalidad para correr a través de un Sistema transacciones de auditoría similares a las operativas, juntamente con los datos reales pero sin afectar los archivos de producción y las salidas normales del proceso". O sea que es un subsistema del Sistema normal, con registros que se mantienen dentro de los archivos perfectamente identificados y con propósitos exclusivos de auditoría. Las salidas de la minicompañia se obtienen en forma separada del resto del proceso normal, aún cuando las transacciones introducidas se procesan junto al conjunto de las reales. La minicompañia prueba la corrección del tratamiento de los datos, aunque no la calidad de los mismos. Debe cumplir tres requisitos:

- Los datos de prueba a preparar deben respetar los diseños y requerimientos de los datos de producción, no debiendo necesitar alteraciones de los programas de producción.
- Se debe conocer perfectamente cuales son los datos que se esperan obtener en cada caso que se introduce.
- Los registros ingresados deben ser ficticios, de forma que puedan luego ser eliminados sin haber afectado los archivos de producción, o bien se debe prever la introducción de otras transacciones que anulen los registros de prueba.

La minicompañia tiene características especiales:

- Es el método más usado; a su vez, puede ser aprovechado por el personal de Sistema para probar modificaciones a programas y por los usuarios para entrenarse en el uso del Sistema.
- Es fácil de usar si se conoce el Sistema, ya que no necesita un conocimiento profundo del equipo.
- Se usa en condiciones reales de operación.
- Puede probar el Sistema completo (procesos manuales y sistemas relacionados), no sólo el procesamiento.
- Es permanente y puede ser reusado.
- No requiere recursos especiales mas allá de los habituales de producción.

Dado lo sensible del entorno en que se realiza la minicompañia, conviene seguir los siguientes pasos para implementarla:

- Obtener la aprobación específica del máximo nivel para utilizarla, explicando detalladamente el método a usar.

- Determinar que método se va a usar, el de los registros fantasmas o el de reversión, de acuerdo a las posibilidades del Sistema.
- Tomar un conocimiento completo sobre el Sistema: objetivos, alcances, manuales de Sistema y Operación, inputs, outputs, uso y frecuencia de las facilidades; también es imprescindible conocer el destino final de los datos que ingresará y los que estos producirán durante el proceso.
- Identificar los formatos de registros que se usan en cada transacción.
- Generar datos válidos y no válidos y preparar una hoja de ruta de cómo se afectarán los datos en el transcurso de la prueba y documentarlos.
- Introducir los datos de auditoría en la corrida normal de los procesos del Sistema.
- Luego de haberse producido la corrida normal, recoger la información de los datos introducidos y proceder a eliminar los registros fantasmas con el método elegido o bien introducir los movimientos de reversión de los datos de prueba; si es necesario, pedir el reproceso de los datos reales una vez eliminados los de prueba.
- Comparar los datos obtenidos con los preestablecidos en la hoja de ruta e informar.

- <u>Beneficios del método de minicompañia:</u>
  - Posibilita que el auditor conozca en forma completa el sistema y su vinculación con la organización.
  - Ayuda a la evaluación de las modificaciones al sistema (60 a 70% del tiempo de las áreas específicas de Sistemas).
  - Permite probar tanto la parte computarizada como la manual y los circuitos intermedios.
  - No depende de ninguna persona o procedimiento en especial.
  - Posibilita tener pruebas regulares de AI sin autorización específica de personas o sectores involucrados, por lo cual permite realizar pruebas sorpresivas.
  - Tiene un costo mínimo.
  - Con el uso permite crear juegos de prueba mas complejos y efectivos.
  - Produce una evidencia objetiva enfatizando la aplicación de políticas y procedimientos de la organización.
  - Su instalación y uso constituye un importante factor disuasivo a cualquier acción no autorizada.
  - Permite evaluar perfomance del sistema aplicativo para casos críticos o extremos.

- <u>Desventajas:</u>

- Si el uso de los registros de prueba, fantasmas o reversibles, no ha sido contemplada en el desarrollo del sistema, se tiene una carga adicional de análisis con cierto margen de error.
- El hecho de declarar cuales van a ser los datos fantasma pone en evidencia la dirección de la Auditoría, aunque no pueda ser evitada.
- No verifica la integridad de los datos, sólo el tratamiento de éstos.
- En el método de reversión, los errores posibles son responsabilidad de los auditores.

XII.3.2 DATOS DE PRUEBA:

Consiste en elaborar lotes de datos de prueba de programas, rutinas o funciones del Sistema auditado, procesándolas en condiciones de laboratorio. Los resultados se comparan con los datos esperados a partir de un cálculo de escritorio. No se usan datos ni condiciones reales, salvo los programas que serán luego pasados a producción. Es una de las técnicas más usadas, dado que no requiere un nivel alto de especialización en el entorno operativo y no implica riesgos a los datos productivos. Se usa antes de poner el Sistema en régimen y durante su vida útil con copias de las bibliotecas operativas.

- Ventajas:
  - Permite familiarizarse fácilmente con la aplicación.
  - Permite pruebas parciales y totales.
  - Al ir aumentando el conocimiento de la aplicación se puede ir enriqueciendo los lotes de prueba.
  - Permite dar un OK fundado antes de la puesta en producción definitiva.
  - Detecta fallas en el control interno antes que se manifiesten con los datos reales.
- Limitaciones:
  - El hecho de ser de laboratorio deja ciertas dudas para la AI, por ejemplo la verificación de si los programas probados son los mismos que se usarán en producción, como responderá el Sistema con una carga importante de datos reales, falta del elemento sorpresa para casos supuestamente delictivos y dificultades en la interface con el usuario que no se presentan en la prueba.
  - Puede consumir muchos recursos del centro de cómputos, con lo cual produce rechazo por el personal del área.
  - El esfuerzo de generación de datos puede ser importante en relación al resultado si se los usa por única vez.
  - En general no involucra al sector usuario, a menos que se logra la colaboración del mismo en la preparación de las pruebas.

XII.3.2 MAPPING:

Consiste en probar el alcance de la prueba de un Sistema y determinar aspectos de la lógica de un programa que no hayan sido probadas. Se utilizan las mismas técnicas del debuging de programación; entre ellas, se puede comprobar:

- Cuales instrucciones del programa se ejecutan y cuales no.
- Cuantas veces se ejecuta cada instrucción.
- Si las instrucciones no ejecutadas constituyen un segmento o procedimiento.
- Si hay pasos que consumen tiempo excesivo de CPU.
- Valores de variables en los pasos intermedios del programa.

  Esta técnica supone un buen manejo de programación del auditor, de manera que pueda discutir con programadores y analistas lo resultados, comparar número de ejecuciones de ciertas sentencias con número de registros procesados y determinar la lógica de las excepciones donde no se ejecutan instrucciones.

- Ventajas:
  - No es muy costoso.
  - Incrementa la eficiencia de la operación por la detección de código no usado por arreglos o mal diseño.
  - La ejecución es simple, se hace agregando la opción de Debug en la corrida.
  - Permite el análisis parcial de subrutinas.
  - Detecta las variables que cambian y se autoarreglan durante la ejecución.
- Limitaciones:
  - Para Sistemas muy complejos resulta impracticable dada la complejidad creciente que produce la concatenación de programas.
  - No comprueba la secuencia correcta de ejecución del programa.
  - No analiza la intención del programa dentro del contexto del Sistema.

XII.3.3 COMPARADORES DE PROGRAMAS:

Consiste en programas que comparan versiones de programas fuente u objeto. Para los fuentes existen utilitarios en los host; para los objetos lo único posible es comparar carácter a carácter. Con ello se logra:

- saber si se han realizado cambios de versiones no autorizados.
- Conocer si hay correspondencia entre objeto y fuente.

- En los fuentes se puede determinar si los cambios introducidos se corresponden con los autorizados.
- Verificar si los programas de las distintas bibliotecas (programador, producción, resguardo) son congruentes en cuanto a versiones.

- Ventajas:
  - Controla una de las principales fuentes de procesamiento irregular: el cambio temporario o permanente de programas.
  - Permite llevar estadísticas de la intensidad del mantenimiento de determinados programas y hacer determinar su grado de obsolescencia.
  - Permite verificar si se están cumpliendo las normas para las modificaciones de programas en producción.
  - Consume pocos recursos y tiempo.

- Desventajas:
  - Esta técnica detecta que los cambios se han efectuado o no, pero no analiza la implicancia de esos cambios.
  - El auditor debe manejar muy bien el lenguaje de programación utilizado.
  - Tampoco da elementos para juzgar el diseño del Sistema.
  - Las modificaciones al lenguaje de máquina no pueden ser detalladas, sólo contadas.
  - Se debe disponer permanentemente de una copia completa de los programas ya auditados para compararlos con una próxima inspección.

XII.3.4 PROCESAMIENTO DUPLICADO:

Consiste en tomar datos reales y procesarlos con programas, rutinas o procedimientos que se realizan especialmente para realizar la misma función que se supone realiza el programa de producción.

Permite verificar el comportamiento del programa en análisis comparando los resultados obtenidos con los reales.
Exige un buen nivel de programación por parte del equipo de AI y un conocimiento acabado del Sistema. Con esta herramienta se consigue:

- Ver si la versión de producción corresponde a la teórica.
- Verificar si los cambios realizados en el programa de producción están produciendo los resultados esperados.
- Comprobar que los procedimientos de evaluación de datos que ingresan en el Sistema son correctos.
- Detecta si la actualización de la documentación del Sistema y sus programas se encuentra actualizada.

Se usa sólo en aplicaciones de alto riesgo y alta complejidad; tiene un costo alto y no provee información sobre la integridad de los datos que se usan.

- Ventajas:
  - Permite realizar una evaluación profunda completamente independiente del centro de cómputos.
  - Permite las pruebas sorpresa.
  - No requiere preparación de datos de prueba, tarea frecuentemente laboriosa y larga.
  - Permite conocer todos los controles que se realizan en el Sistema y su efectividad.
- Desventajas:
  - Frecuentemente para reducir los altos costos de desarrollo de esta aplicación se usan copias de los programas originales, lo que puede duplicar errores al no interpretarse la codificación.
  - Implica efectuar modificaciones al programa para proceso duplicado cada vez que se realizan en producción.
  - Los datos reales que se usan frecuentemente no contemplan todas las variantes de proceso que el programa soporta, especialmente los valores extremos; por ello el resultado correcto sólo se refiere al entorno instantáneo.

XII.3.5 TAGGING:

Consiste en agregar un identificador a una transacción. El identificador o tag sirve par identificar esa transacción en puntos prefijados y durante toda el procesamiento de la aplicación, proporcionando una pista de auditoría especial respecto a la circulación de la transacción tagged.

Por ej.: el auditor puede marcar todos los créditos superiores a un cierto monto, o todos los adelantos de sueldo pedidos antes de una cierta fecha, o la totalidad del monto facturado para un grupo de ítems, etc. Luego esa información se recoge en un listado especial para AI.

El tagging se puede hacer con una marca fisica en un registro o una rutina o procedimiento por el cual el programa seleccione determinados registros y los grabe aparte o los separe de otra forma (ej.: un índice especial).

Esta técnica permite verificar procedimientos completos, donde actúen varios programas interactivos o batch, pudiendo ser combinados con procesos manuales ya que se analiza el resultado final del ciclo de procesamiento desde el momento del marcado. No necesita de una gran especialización por parte del auditor, aunque sí un buen conocimiento del proceso de datos del o los aplicativos en los que interviene el tagging.

XII.3.5 SNAPSHOT:

Se basa en hacer un vuelco del valor en memoria de todas las variables en estudio en uno o varios momentos de una aplicación. Ello permite hacer el walk-through de los valores buscados. La técnica implica tomar una fotografia de una transacción a medida que fluye por el sistema y es similar a los dump que se hacen en programación.

Puede producirse por indicaciones en el procedimiento de ejecución (lenguaje de control) o por decisión interactiva del auditor.

Es muy útil para el rastreo durante las corridas de producción, sean batch o interactivas, sin alterar los datos, pero muy complejas de leer y exigen una gran pericia de parte del auditor.

El procedimiento a seguir para aplicar un snapshot:

1) Determinar los momentos en el proceso que se aplicará el snapshot.
2) Incorporación de las rutinas o procedimientos a los programas de producción.
3) Preparación del programa para leer o listar los datos disparados. En algunos sistemas operativos existen utilitarios para editar los dumps.
4) Determinar los puntos del snapshot. Es el punto más importante; debe establecerse en entre el momento de ingreso de las transacciones al sistema y cuando abandona el segmento a analizar, ubicando los puntos de decisiones claves y donde se forman o se consolidan registros.
5) Forma en que se identifican las variable a examinar y el momento en que se hace: puede ser por activación de las rutinas al ejecutarse todas las transacciones de un cierto tipo (créditos, débitos, ajustes, etc.), activación por determinadas condiciones paramétricas (ventas a plazo para clientes tipo A), activación por el paso de la transacción por un determinado punto de la aplicación (suma a un total) y combinaciones de las tres.

6) Diseñar los archivos de snapshot donde se guarden los datos que se recogerán en los distintos puntos de la aplicación donde se dispare el snapshot, para luego ser impresa o resumida.
7) Individualización del snapshot, para el caso frecuente que una transacción atraviese más de una vez, la transacción se debe poder identificar junto con el valor de la variable en ese punto. Por ello, el listado de snapshot debe incluir las claves del registro, el programa que originó el vuelco y fecha y hora del vuelco.
8) Si el formato de salida es correctamente elaborado desde su proceso del archivo de snapshot, esto disminuye notablemente la necesidad de especialización del auditor. También se usan utilitarios como el ACL.

- Ventajas:

  - Permite un análisis de la información casi sin posibilidad de ser alterada en el proceso
  - Puede repetirse indefinidamente
  - Permite detectar tanto fallas operativas como intencionales

- Desventajas:

  - Grado de especialización necesario del auditor
  - Análisis de la información complicada
  - Instrumentación costosa
  - Debe emplearse concurrente con otras técnicas para poder lograr un análisis que haga a toda la estructura del sistema

XII.3.6 SYSTEM CONTROL AUDIT REVIEW FILE:

SCARF implica la inserción de módulos de AI en los programas de una aplicación para lograr un monitoreo permanente de las transacciones procesadas por el sistema. Los módulos son ubicados en puntos predeterminados para acumular información de interés para la AI en el archivo SCARF, desde donde el auditor revisa periódicamente para investigar las excepciones que allí detecta.

Su implementación debe hacerse preferiblemente desde el diseño del sistema, donde se debe establecer cual será la información a recoger y la modalidad de actualización del archivo SCARF. La información que más frecuentemente se recoge es:

- Errores producidos por la aplicación, generalmente por fallas en el diseño del sistema.
- Cumplimiento de los procedimientos en vigencia, por ejemplo: rebajas por cantidad, tasas de interés, etc.

- Excepciones del sistema: para errores que caen dentro del margen de tolerancia pero pueden ser riesgosos en su repetición.
- Muestras estadísticas: para dar evaluaciones de eficiencia o carga operativa.

SCARF es la técnica más aplicada cuando se logra introducir la AI en el diseño. Su único inconveniente es que puede degradar la perfomance del sistema.

XII.3.7 TRACING:

Consiste básicamente en hacer un Trace del programa, con las herramientas que ofrece el mismo compilador. Se usa excepcionalmente y fundamentalmente para lenguajes de bajo nivel.

Su gran complejidad de análisis requiere una gran especialización y sólo se justifica cuando las restantes técnicas no dan resultados confiables.

XII.4 COBIT:

Es la primer norma de nivel internacional aceptada para la AI. Su uso se extiende a prácticamente todo el mundo, tratando fundamentalmente de dar pautas para que los resultados de las Auditorías sean mensurables con exactitud y comparables.

XII.4.1 DETERMINACIÓN DE LOS OBJETIVOS DE CONTROL

En esta etapa se definen los objetivos de control que nos proporciona el marco metodológico formal COBIT (Objetivos de Control Para la Información y Tecnologías Afines), que está ampliamente aceptado por la comunidad internacional de auditores de sistemas de información como una norma estándar.

La metodología COBIT será la herramienta de análisis durante la ejecución de una auditoría.

XII.4.2 MARCO METODOLÓGICO COBIT:

Definiciones:

- **Control**: se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

- **Objetivo de Control:** Un objetivo de Control en Tecnología de Información (TI) es una definición del resultado o propósito, que se desea alcanzar implementando procedimientos de control específicos dentro de cualquier actividad relacionada con las tecnologías de Información (TI) (mediante la implementación de 302 detallados y específicos a través de los 34 procesos de TI).

- **Características Generales:**

    - Es importante mencionar la Misión de COBIT: "Investigar, Desarrollar, Publicar y Promover un conjunto de Objetivos de Control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores".
    - COBIT se ha desarrollado como norma "aplicable y generalmente aceptada" de buenos usos y costumbres de control de las Tecnologías de la información. El término "aplicable y generalmente aceptado" se utiliza con el mismo sentido que "principios de contabilidad generalmente aceptados". Para los objetivos del proyecto los "buenos usos y costumbres" se entiende como el consenso entre los expertos.
    - La norma es relativamente pequeña y pretende, donde sea posible, ser pragmática y responder a las necesidades empresariales, a la vez de ser independiente de las plataformas técnicas adoptadas en las organizaciones.
    - El producto COBIT utiliza Objetivos de Control mejorados con estándares específicos de tipo técnico, profesional, normativo e industrial existentes y emergentes; estos objetivos de control se han desarrollado para su aplicación en el amplio espectro de sistemas de información en las empresas.
    - Por lo tanto, COBIT está orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnologías de información y con tecnologías relacionadas.
    - COBIT proporciona un conjunto de 34 Objetivos de Control de Alto nivel, uno para cada uno de los procesos de TI, agrupados en cuatro dominios ***(ver ANEXO 4).-***