UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

SEGURIDAD DE LA INFORMACIÓN EN MEDIOS DE ALMACENAMIENTO MASIVO

T E S I S

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

ERNESTO ALONSO VILLEGAS JIMENEZ

ASESOR DE TESIS:

ING. RODOLFO VÁZQUEZ MORALES

SAN JUAN DE ARAGÓN, EDO DE MÉXICO 2008

AGRADECIMIENTO

GRACIAS

A MI FAMILIA

POR TODO EL APOYO RECIBIDO

POR LA PACIENCIA QUE HAN TENIDO

POR LA SANGRE QUE HEREDE

¡GRACIAS A TODOS LES DOY LAS GRACIAS!

LA VERDAD ESTÁ ABIERTA
A TODOS LOS HOMBRES.

NECA.

DEDICATORIA

A TI

HOMBRE DE CABELLO CRESPO QUE EN TUS PALABRAS LLEVAS LA SABIDURIA DE LA EXPERIENCIA.

MUJER DE PIEL CANELA QUE EN TU GENÉTICA BRINDAS TRIUNFO Y VALOR A TU DESCENDENCIA.

NIÑA DE OJOS CLAROS Y CRISTALINOS QUE LUCHAS CON RISAS, ENOJO Y LLANTO POR TU SANGRE.

NIÑO DE MIRADA PROFUNDA Y GRANDES IDEALES POR CUMPLIR.

QUE CON GOLPES, DESPRECIO, INSULTOS, ENVIDIA Y RENCOR; ME IMPULSASTE A SEGUIR ADELANTE.

QUE CON AMOR, CARIÑO, COMPRENSIÓN, APOYO Y CONFIANZA; ME DISTE ARMAS PARA LUCHAR.

A TI

CON AMOR Y RESPETO.

ERNESTO ALONSO

ÍNDICE PÁGINA

INTRODUCCIÓN

Hoy día todos los habitantes del mundo somos dependientes directos o indirectos del uso de las computadoras. El avance tecnológico en el área informática; desde su primera generación (1924: consolidación de IBM) hasta nuestros días (2008: el microprocesador de 64 bits), ha creado en el ser humano la necesidad imperiosa del uso de los sistemas informáticos, el manejo de datos (información) se ha convertido en uno de los factores primordiales en el desarrollo de la era computacional.

Diariamente estamos en continua relación con los medios digitales (desde un simple celular, hasta un complejo sistema computacional), y es así como nos vemos sumergidos en un mundo de datos del cual pasamos a formar parte inconsciente o conscientemente.

Dada esta relación se deben tratar estos de forma segura, así mismo es recomendable clasificarlos, distribuirlos y almacenarlos adecuada y eficientemente, ya que es muy importante no perder información en cada una de estas etapas, pues esto podía ocasionar problemas muy severos en el momento de tratar de consultar dicha información.

Por tal motivo es conveniente implementar una investigación de tipo descriptiva para expresar las diferentes técnicas que existen para manipular datos, y conocer los métodos pertinentes para clasificarlos, distribuirlos y almacenarlos de forma segura, para evitar pérdidas de información, pues dada la cantidad de información que actualmente se utiliza (personal o industrialmente), es significativo hacer hincapié en el valor que intangiblemente representan estos datos, por tal motivo debemos salvaguardar este bien que para su creación necesita demasiado tiempo de trabajo (horas hombre). Dicho lo anterior, se debe considerar en primer plano la seguridad de la información en medios de almacenamiento masivo.

Para poder realizar este trabajo de tesis se considerarán los siguientes capítulos:

- CAPÍTULO 1

ENTORNO DE LOS SISTEMAS DE INFORMACIÓN.

- CAPÍTULO 2

IMPORTANCIA DE LA INFORMACIÓN.

- CAPÍTULO 3

MANUAL DE PROCEDIMIENTOS, TÉCNICAS Y MÉTODOS ESPECIALIZADOS BASADO EN LA NORMA ISO/IEC 27001:2005.

CONCLUSIONES.
BIBLIOGRAFÍA.
GLOSARIO.
ANEXO

Con el tema:

"SEGURIDAD DE LA INFORMACIÓN EN MEDIOS
DE ALMACENAMIENTO MASIVO".

CAPÍTULO 1

ENTORNO DE LOS SISTEMAS DE INFORMACIÓN.

INTRODUCCIÓN

Podemos entender como seguridad un estado de cualquier sistema (informático o no) que nos indica que se encuentra libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de Seguridad de la Información es utópico porque no existe un sistema 100% seguro. Para que un sistema informático se pueda considerar como seguro debe tener estas cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado y debe encontrarse completa.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la misma, ya que en la actualidad la información es manipulada en distintos Sistemas de Información que presentan diferentes esquemas de operación con parámetros definidos y estandarizados, así mismo con diversas infraestructuras y riesgos de trabajo.

1.1 SISTEMAS DE INFORMACIÓN.

1.1.1 DESCRIPCIÓN DE UN SISTEMA DE INFORMACIÓN.

El estudio de los Sistemas de Información se originó como una sub-disciplina de las ciencias de la computación en un intento por entender y racionalizar la administración de la tecnología dentro de las organizaciones.

Los Sistemas de Información han madurado hasta convertirse en un campo de estudios superiores dentro de la administración. Adicionalmente, cada día se enfatiza más como un área importante dentro de la investigación en los estudios de administración, y es enseñado en las universidades y escuelas de negocios más grandes en todo el mundo.

En la actualidad, la Información y la tecnología de la Información forman parte de los cinco recursos con los que los ejecutivos crean y/o modelan una organización, junto con el personal, dinero, material y maquinaria.

Muchas compañías han creado la posición de Director de Información (CIO, por sus siglas en inglés *Chief Information Officer*) quien asiste al comité ejecutivo de la compañía, junto con el Director Ejecutivo, el Director Financiero, el Director de Operaciones y el Director de Tecnología (es común que el Director de Información actúe como Director de Tecnología y viceversa), observemos la siguiente imagen que nos muestra la evolución de los Sistemas de Información a lo largo del tiempo (Figura 1).

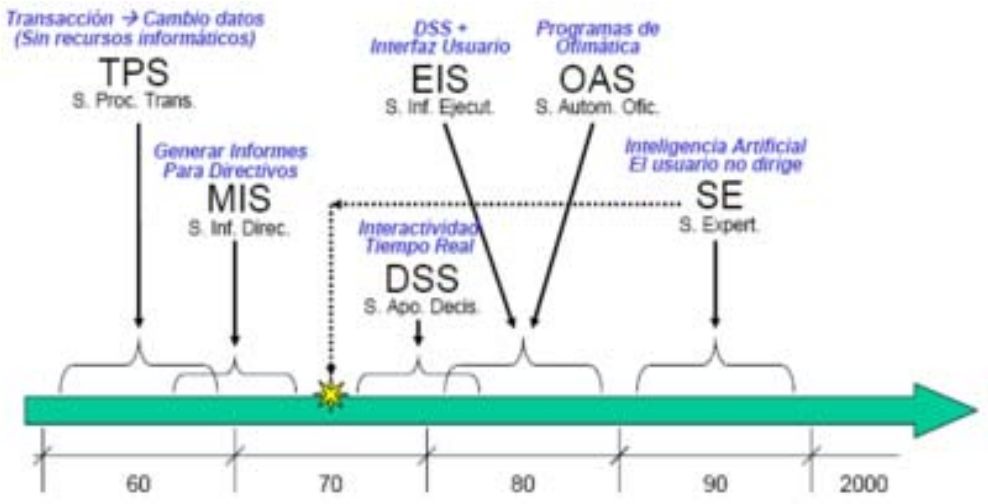


Figura 1: Evolución de los SI.

Un **sistema de información** (SI)[1] es un conjunto organizado de elementos, estos elementos son de 4 tipos:

- Personas.
- Datos.
- Actividades o técnicas de trabajo.
- Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).

Todo ese conjunto de elementos interactúan entre si para procesar los datos y la información (incluyendo procesos manuales y automáticos) y distribuirla de la manera más adecuada posible en una determinada organización en función de sus objetivos.

Normalmente el término es usado de manera errónea como sinónimo de sistema de información informático, estos son el campo de estudio de la tecnología de la información (IT), y aunque puedan formar parte de un sistema de información (como recurso material), por sí solos no se pueden considerar como

[1] http://www.itson.mx/dii/jgaxiola/sistemas/introduccion.html#conceptos 10/09/08

sistemas de información, este concepto es más amplio que el de sistema de información informático.

No obstante un sistema de información puede estar basado en el uso de computadoras, según la definición de Langefors[2] este tipo de sistemas son:

- Un medio implementado tecnológicamente para grabar, almacenar y distribuir expresiones lingüísticas,
- así como para extraer conclusiones a partir de dichas expresiones.

El término **Sistemas de Información** tiene diferentes significados:

En seguridad computacional, un sistema de información está descrito por tres componentes:

Estructura:

- Repositorios, que almacenan los datos permanente o temporalmente, tales como "buffers", RAM (memoria de acceso aleatorio), discos duros, caché, etc.
- Interfaces, que permiten el intercambio de información con el mundo no digital, tales como teclados, altavoces, monitores, escáneres, impresoras, etc.

Canales, que conectan los repositorios entre si, tales como "buses", cables, enlaces inalámbricos, etc. Una red de trabajo es un conjunto de canales físicos y lógicos.

[2] Langefors, Börje (1973). *Theoretical Analysis of Information Systems*. Auerbach.

Comportamiento:

- Servicios, los cuales proveen algún valor a los usuarios o a otros servicios mediante el intercambio de mensajes.
- Mensajes, que acarrean un contenido o significado hacia los usuarios o servicios.

Características de los sistemas de información modernos:

- ✓ Sistemas sencillos sirviendo a funciones y niveles múltiples dentro de la empresa.
- ✓ Acceso inmediato en línea a grandes cantidades de información.
- ✓ Fuerte confiabilidad en la tecnología de telecomunicaciones.
- ✓ Mayor cantidad de inteligencia y conocimientos implícita en los sistemas.
- ✓ La capacidad para combinar datos y gráficas.

Actualmente, los sistemas de información cumplen dentro de las organizaciones tres objetivos básicos.

- ✓ Automatización de procesos operativos. (Sistemas transaccionales)
- ✓ Proporcionar información que sirva de apoyo al proceso de la toma de decisiones. (Sistemas de soporte a las decisiones)
- ✓ Lograr ventajas competitivas a través de su implementación y uso.(Sistemas estratégicos)

1.1.2 OBJETIVO DE UN SISTEMA DE INFORMACIÓN.

Dependiendo del tipo de sistema de información que se esté tratando, las funciones esenciales que respaldan su existencia se verán modificadas. En general, los sistemas de información tienen como objetivo:

- ➢ Respaldar las operaciones empresariales.
- ➢ Respaldar la toma de decisiones gerenciales.
- ➢ Respaldar la ventaja competitiva estratégica.

- Contribuir a la automatización de actividades y procesos en las empresas.
- Llevar la información de manera oportuna y adecuada a las instancias de la empresa que así lo requieran.
- Proporcionar un diagnóstico de la empresa en un momento dado.

Dar elementos de juicio para realizar pronósticos para la empresa. Un sistema de información ejecuta tres actividades generales. En primer lugar, recibe datos de fuentes internas o externas de la empresa como elementos de entrada. Después, actúa sobre los datos para producir información. Por último el sistema produce la información para el futuro usuario, que posiblemente sea un gerente, un administrador o un miembro del cuerpo directivo. La evaluación de la información obtenida permite la retroalimentación del sistema.

1.1.3 CLASIFICACIÓN GENERAL DE LOS SISTEMAS DE INFORMACIÓN[3].

A. Transaccionales. (Sistemas transaccionales)

Las principales características son:

- ✓ A través de éstos suelen lograrse ahorros significativos de mano de obra.
- ✓ Normalmente son el primer tipo de SI que se implanta en las organizaciones.
- ✓ Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- ✓ Tienen la propiedad de ser recolectores de información.
- ✓ Son fáciles de justificar ante la dirección ya que sus beneficios son visibles y palpables.

B. Sistemas de Apoyo a las decisiones (Sistemas de Soporte a las Decisiones, Sistemas Gerenciales o Sistemas Ejecutivos, Sistema de Soporte para la Toma de Decisiones en Grupo.)

[3] http://www.itson.mx/dii/jgaxiola/sistemas/introduccion.html#conceptos 10/09/08

- ✓ Suelen introducirse después de haber implantado los sistemas transaccionales.
- ✓ Suelen ser intensivos en cálculos y escasos en entradas y salidas de información.
- ✓ La información que generan sirve de apoyo a los mandos intermedios y de alta administración en el proceso de la toma de decisiones.
- ✓ No suelen ahorrar mano de obra.
- ✓ La justificación económica para el desarrollo de estos sistemas es difícil.
- ✓ Suelen ser SI interactivos y amigables, con altos estándares de diseño gráfico y visual, ya que están dirigidos al usuario final.
- ✓ Apoyan la toma de decisiones que por su naturaleza son repetitivas.
- ✓ Pueden ser desarrollados directamente por el usuario final sin la participación operativa de los analistas.

C. Sistemas Estratégicos: (Sistemas Expertos (ES), Sistemas Estratégicos)

Su función principal no es apoyar a la automatización de procesos operativos ni proporcionar información para la toma de decisiones. Sin embargo, este tipo de sistemas puede llevar a cabo dichas funciones.

- ✓ Suelen desarrollarse "in house".
- ✓ Típicamente su forma de desarrollo es a base de incrementos y a través de su evolución permanente dentro de la organización.
- ✓ Su función es lograr ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores.
- ✓ Apoyan el proceso de innovación dentro de la empresa.

Elementos de un sistema de Información (Figura 2):

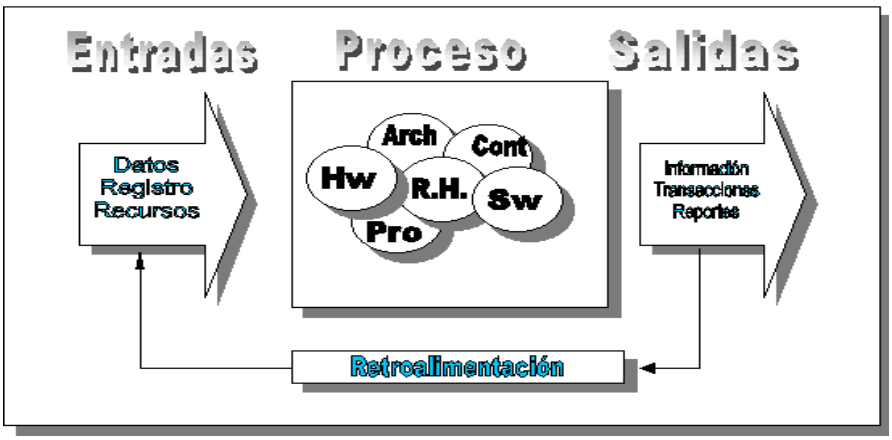


Figura 2

1.1.4 APLICACIÓN DE LOS SISTEMAS DE INFORMACIÓN.

Los sistemas de información tratan el desarrollo, uso y administración de la infraestructura de la tecnología de la información en una organización.

En la era post-industrial, la era de la información, el enfoque de las compañías ha cambiado de la orientación hacia el producto a la orientación hacia el conocimiento, en este sentido el mercado compite hoy en día en términos del proceso y la innovación, en lugar del producto. El énfasis ha cambiado de la calidad y cantidad de producción hacia el proceso de producción en sí mismo, y los servicios que acompañan este proceso.

El mayor de los activos de una compañía hoy en día es su información, representada en su personal, experiencia, conocimiento, innovaciones (patentes, derechos de autor, secreto comercial). Para poder competir, las organizaciones deben poseer una fuerte infraestructura de información, en cuyo corazón se sitúa la infraestructura de la tecnología de la información.

De tal manera que el sistema de información se centre en estudiar las formas para mejorar el uso de la tecnología que soporta el flujo de información dentro de la organización.

1.1.5 ÁREAS DE TRABAJO.

El trabajo con los sistemas de información puede centrarse en cualquiera de estas tres áreas generales:

- Estrategia de los sistemas de información.
- Gestión de los sistemas de información.
- Desarrollo de los sistemas de información.

Cada una de estas ramas se subdivide a su vez en disciplinas que se traslapan con otras ciencias y con otras disciplinas de la administración tales como ciencias de la computación, ingenierías, ciencias sociales y ciencias del comportamiento y la administración de negocios.

1.2. NORMA ISOIEC27001.

Actualmente los Sistemas de Información se encuentran sujetos a normas que proponen la implementación de procesos estudiados y estandarizados para poder minimizar las fallas físicas, lógicas y humanas a las que están propensos, puesto que; la norma ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña, es la mejor opción para trabajar con los Sistemas de Información.

1.2.1 NOMBRE DE LA ISO[4].

El “International Organization for Standardization” tendría diversas siglas en diversas idiomas (“IOS” en inglés, “OIN” en francés para la *organización internationale de normalisation*), sus fundadores decidían darle también un nombre corto, de uso múltiple. Eligieron la **“ISO”**, derivada de los *isos* griegos,

[4] http://www.iso.org

significando el “igual”. Lo que el país, lo que la lengua, la forma corta del nombre de organización es siempre ISO.

La ISO es los estándares más grandes del mundo que desarrollan la organización. Entre 1947 y el hoy, la ISO ha publicado más de 17000 estándares internacionales, extendiéndose de los estándares para las actividades tales como agricultura y construcción, con la ingeniería industrial, a los aparatos médicos, a los progresos de tecnología de la información muy reciente.

Dado el alcance multisectorial de la organización, sería duro presentar una perspectiva histórica que resume los desafíos, la pasión, los logros excepcionales o, a veces, las oportunidades perdidas, en la variedad grande de sectores cubiertos por el trabajo técnico de la ISO.

Por lo tanto hemos elegido destacar los marcadores dominantes en la historia de la organización de una perspectiva general.

Fundación.

La ISO nació de la unión de dos organizaciones - el AIA (federación internacional del nacional que estandariza asociaciones). Establecido en Nueva York en 1926, y el UNSCC (comité de coordinación de los estándares de Naciones Unidas), establecido en 1944.

En octubre de 1946, los delegados a partir de 25 países, encontrándose en el instituto de ingenieros civiles en Londres, decidían crear una nueva organización internacional, cuyo el objeto sería “facilitar la coordinación y la unificación internacional de estándares industriales”. La nueva organización, ISO, comenzó oficialmente operaciones el 23 de febrero de 1947.

1.2.2 ANTECEDENTES DE LA NORMA ISOIEC27001.

ORIGEN[5].

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de

[5] http://www.iso27000.es/ 05/05/08

Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

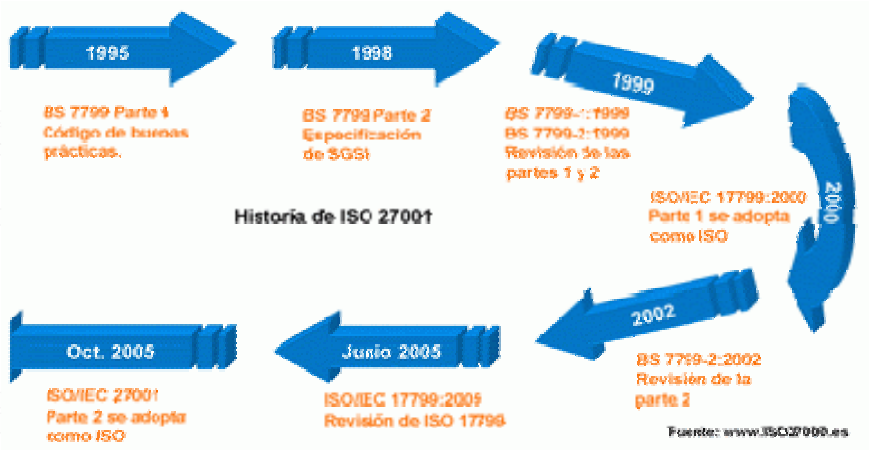


Figura 3

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

LA SERIE 27000.

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

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

- ISO 27001: Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la

cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR. Otros países donde también está publicada en español son, por ejemplo, Colombia , Venezuela y Argentina. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

- ISO 27002: Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

- ISO 27003: En fase de desarrollo; su fecha prevista de publicación es mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ISO 27004: En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- ISO 27005: En fase de desarrollo; su fecha prevista de publicación es mayo de 2008. Consistirá en una guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Recogerá partes de ISO/IEC TR 13335.

- ISO 27006: Publicada el 1 de marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoria y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoria de un SGSI.

- ISO 27011: En fase de desarrollo; su fecha prevista de publicación es Enero de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- ISO 27031: En fase de desarrollo; su fecha prevista de publicación es mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- ISO 27032: En fase de desarrollo; su fecha prevista de publicación es febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

- ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028.

- ISO 27034: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.

- ISO 27799: En fase de desarrollo; su fecha prevista de publicación es 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

1.2.3 OBJETIVO.

Su objetivo principal es el establecimiento e implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Los siguientes objetivos particulares son los que persigue un SGSI:

- La definición clara y transmitida a toda la organización de los objetivos y directrices de seguridad.

- La sistematización, objetividad y consistencia a lo largo del tiempo en las actuaciones de seguridad.

- El análisis y prevención de los riesgos en los Sistemas de Información.

- La mejora de los procesos y procedimientos de gestión de la información.
- La motivación del personal en cuanto a valoración de la información.
- El cumplimiento con la legislación vigente.
- Una imagen de calidad frente a clientes y proveedores.
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorias externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.

- Aumento de la motivación y satisfacción del personal.

- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.2.4 CAMPO DE APLICACIÓN.

No está enfocado solo a grandes empresas, sino que deberá ser aplicado en las PYMES que deseen trabajar como socias de negocio de cualquier otra grande o pequeña empresa.

Actualmente es el único estándar aceptado internacionalmente para la administración de la Seguridad de la Información y se aplica a todo tipo de organizaciones, independientemente de su tamaño o actividad.

1.2.5 REFERENCIAS.

CONTENIDO[6].

En esta sección se hace un breve resumen del contenido de las normas ISO 27001, ISO 27002 e ISO 27006.

ISO 27001:2005.

- Introducción: generalidades e introducción al método PDCA.

- Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.

- Normas para consulta: otras normas que sirven de referencia.

- Términos y definiciones: breve descripción de los términos más usados en la norma.

[6] http://www.iso27000.es/doc_iso27000_all.htm 05/05/08

- Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.

- Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

- Auditorias internas del SGSI: cómo realizar las auditorias internas de control y cumplimiento.

- Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

- Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.

- Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.

- Relación con los Principios de la OCDE: anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.

- Correspondencia con otras normas: anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.

- Bibliografía: normas y publicaciones de referencia.

ISO 27002:2005 (anterior ISO 17799:2005)

- Introducción: conceptos generales de seguridad de la información y SGSI.

- Campo de aplicación: se especifica el objetivo de la norma.

- Términos y definiciones: breve descripción de los términos más usados en la norma.

- Estructura del estándar: descripción de la estructura de la norma.

- Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

- Política de seguridad: documento de política de seguridad y su gestión.

- Aspectos organizativos de la seguridad de la información: organización interna; terceros.

- Gestión de activos: responsabilidad sobre los activos; clasificación de la información.

- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; computadoras portátiles y teletrabajo.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las

aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.

- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorias de los sistemas de información.

- Bibliografía: normas y publicaciones de referencia.

ISO 27006:2007.

(Esta norma referencia directamente a muchas cláusulas de ISO 17021 -requisitos de entidades de auditoria y certificación de sistemas de gestión-, por lo que es recomendable disponer también de dicha norma, que puede adquirirse en español en AENOR).

- Preámbulo: presentación de las organizaciones ISO e IEC y sus actividades.

- Introducción: antecedentes de ISO 27006 y guía de uso para la norma.

- Campo de aplicación: a quién aplica este estándar.

- Referencias normativas: otras normas que sirven de referencia.

- Términos y definiciones: breve descripción de los términos más usados en la norma.

- Principios: principios que rigen esta norma.

- Requisitos generales: aspectos generales que deben cumplir las entidades de certificación de SGSIs.

- Requisitos estructurales: estructura organizativa que deben tener las entidades de certificación de SGSIs.

- Requisitos en cuanto a recursos: competencias requeridas para el personal de dirección, administración y auditoria de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratas.

- Requisitos de información: información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.

- Requisitos del proceso: requisitos generales del proceso de certificación, auditoria inicial y certificación, auditorias de seguimiento, recertificación, auditorias especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.

- Requisitos del sistema de gestión de entidades de certificación: opciones, opción 1 (requisitos del sistema de gestión de acuerdo con ISO 9001) y opción 2 (requisitos del sistema de gestión general).

- Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector: potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.

- Anexo B - Áreas de ejemplo de competencia del auditor: consideraciones de competencia general y consideraciones de competencia

específica (conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGSIs).

- Anexo C - Tiempos de auditoria: introducción, procedimiento para determinar la duración de la auditoria y tabla de tiempos de auditoria (incluyendo comparativa con tiempos de auditoria de sistemas de calidad -ISO 9001- y medioambientales -ISO 14001-).

- Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005: tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

1.3. DISPOSICIONES GENERALES.

La siguiente tabla muestra los artículos en los que se basa nuestro estudio, que son extracto de la serie de normas ISO/IEC 27000:

Ref.	Objetivo	Consejos de implementación	Posibles métricas
4. Evaluación y tratamiento de riesgos[7]			
4.1	Evaluación de riesgos de seguridad	Se puede usar cualquier método de gestión de riesgos de seguridad de la información, con preferencia por métodos documentados, estructurados y generalmente aceptados como OCTAVE, MEHARI, ISO TR 13335 ó BS 7799 Parte 3 (y, en su momento, ISO/IEC 27005).	Porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".

[7] http://sociedaddelainformacion.wordpress.com/2007/02/25/la-familia-de-normas-isoiec-27000/ 19/05/08

4.2	Tratamiento de riesgos de seguridad	La gerencia (específicamente, los propietarios de activos de in-formación) necesita evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones deben documentarse en un Plan de Tratamiento de Riesgos (PTR). Es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información que se estiman dentro de la "tolerancia al riesgo" de la organización, sin que sea éste el enfoque por defecto.	Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia. Costes de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI. Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios.
5. Política de seguridad[8]			
5.1	Política de seguridad de la información	Piense en términos de un manual o wiki de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoria, gerencia o autoevaluación).

[8] http://cibsi05.inf.utfsm.cl/presentaciones/empresas/Neosecure.pdf 19/05/08

6. Aspectos organizativos de la seguridad de la información[9]			
6.1	Organización interna	Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y *Compliance*.	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.
6.2	Terceros	Haga inventario de conexiones de red y flujos de información significativos con 3as partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos. ¡Esto puede dar miedo, pero es 100% necesario! Considere exigir certificados en ISO/IEC 27001 a los *partners* más críticos, tales como *outsourcing* de TI, proveedores de servicios de seguridad TI, etc.	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.
7. Gestión de activos[10]			
7.1	Responsabili-dad sobre los activos	Elabore y mantenga un inventario de activos de información (similar al preparado en su día para el *Efecto 2000*), mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y

[9] http://ftp.ucv.ve/Documentos/Congreso2008/Ponencias%20Martes%20110308/05.%20doc_iso27000_all.pdf 19/05/08
[10] http:// www.ISO27001security.com

		relevantes (p. Ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.). Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.	para mantener dichos riesgos en niveles aceptables.
7.2	Clasificación de la información	¡Mantenga la sencillez! Distinga los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo. Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad.	Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").
8. Seguridad ligada a los recursos humanos[11]			
8.1	Antes de la contratación	Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia,	Porcentaje de nuevos empleados o *pseudoempleados* (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

[11] http://www.ISO27001security.com

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

		estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).	
9. Seguridad física y ambiental[12]			
9.1	Áreas seguras	El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. Ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. Ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta,	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

[12] http://www.iso27000.es

		reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.	
9.2	Seguridad de los equipos	Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita. Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc. Tome en consideración el uso de códigos de barras para hacer los chequeos más eficientes.	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.
10. Gestión de comunicaciones y operaciones[13]			
10.1	Responsabilida-des y procedimientos de operación	Documente procedimientos, normas y directrices de seguridad de la	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado

[13] ISO27001security forum

		información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización.	parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-).
10.2	Gestión de la provisión de servicios por terceros	¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema de supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio. Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. En algunos casos puede funcionar un sistema de premio y castigo. Esté atento a cambios que tengan impacto en la seguridad.	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.
10.3	Planificación y aceptación del sistema	Adopte procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, etc., usando estándares aceptados como ISO 20000 (ITIL) donde sea posible. Defina e imponga estándares de seguridad básica (mínimos aceptables) para todas las plataformas de sistemas operativos, usando las	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similares y (b) cuya conformidad con dichos estándares ha sido comprobada mediante *benchmarking* o pruebas.

		recomendaciones de seguridad de CIS, NIST, NSA y fabricantes de sistemas operativos y, por supuesto, sus propias políticas de seguridad de la información.	
10.4	Protección contra código malicioso y móvil	Combine controles tecnológicos (p. Ej., software antivirus) con medidas no técnicas (educación, concienciación y formación). ¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables!	Tendencia en el número de virus, gusanos, troyanos o *spam* detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.
10.5	Copias de seguridad	Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.	Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.

		Encripte copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?).	
10.6	Gestión de la seguridad de las redes	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.
10.7	Manejo de los soportes	Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Encripte todos los datos sensibles o valiosos antes de ser transportados.	Porcentaje de soportes de backup o archivo que están totalmente encriptados.
10.8	Intercambio de información	Estudie canales de comunicaciones alternativos y "preautorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones *offline* por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.
10.9	Servicios de comercio electrónico	Trabaje estrechamente con las unidades de negocio para desarrollar un	"Estado de la eSeguridad", es decir, un informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de

		eBusiness seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de eCommerce, desde el principio (también en cualquier cambio/actualización posterior). Insista en el valor añadido de la seguridad en la reducción de riesgos comerciales, legales y operativos asociados al eBusiness. Trabaje los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad.	penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas, cambios planificados, etc.
10.10	Supervisión	El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico. Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.	Porcentaje de sistemas cuyos *logs* de seguridad (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de *logs* y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los *logs* de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.

Tabla 1

CAPÍTULO 2

IMPORTANCIA DE LA INFORMACIÓN.

INTRODUCCIÓN

El ser humano y lo que produce (estadísticamente) con el paso del tiempo se ha convertido en un dato y por este motivo es indefectible considerar la valía que estos tienen para nosotros.

En la actualidad es muy fácil almacenar datos, ya que la tecnología nos ha brindado la oportunidad de tener dispositivos capaces de guardar cantidades inmensas de información (Terabytes), para efectos de nuestro estudio consideraremos únicamente a los medios de almacenamiento masivo de datos conocidos como Discos Duros o Hard Disk, por tanto son los que aun con la revolución tecnológica que vivimos se mantienen insustituibles por las características que los distinguen de los demás medios de almacenamiento masivo.

¿Por qué es importante mantener a salvo la información recabada en medios de almacenamiento masivo?

En repetidas ocasiones hemos visto personas lamentándose (en cualquier estrato social donde se tiene contacto con algún dispositivo capaz de almacenar y procesar datos), por la pérdida de cualquier archivo por importante o no que este sea, debido a que, en la mayoría de los casos no se tienen el conocimiento mínimo que se requiere para manipularlos.

Esto ocurre a frecuentemente nivel personal y por lo general no tiene efectos colaterales muy significativos; pero a nivel empresarial o industrial le costaría el empleo a una o varias personas y puede incluso, llevar a la ruina a la empresa o industria que se vea afectada por estos errores, que por lo general son humanos.

2.1 IMPORTANCIA DE LA INFORMACIÓN.

Como lo hemos venido mencionando, la información además de ser el principal activo de las empresas y las personas, se ha convertido en el principal medio de difusión de hechos, acontecimientos y prácticamente la vida del ser humano (representa la vida cotidiana, presente, pasado y futuro) y dada tal importancia es necesario presentar las principales propiedades que debe cumplir la información para pertenecer a los sistemas de información:

1. Pertinente (Útil):

La información pertinente es útil y contribuye a las necesidades y circunstancias peculiares del administrador. La información no pertinente es inútil y hasta puede estorbar el desempeño de un administrador ocupado que tiene que dedicar tiempo valioso a determinar si la información es pertinente.

Dados los gigantes volúmenes de información a los que están expuestos los administradores de nuestros días, y dadas las limitaciones de las facultades humanas para procesar información, quienes diseñan los sistemas de información deben cerciorarse de que los administradores reciben sólo información pertinente.

2. Oportuna (Tiempo Justo):

Lo que debemos garantizar es que llegue en el momento oportuno. Para que una información se pueda utilizar, deberá estar disponible

- Se utilice cuando sea necesario (Antes de tomar decisiones).
- Que esté al alcance de sus usuarios y destinatarios
- Se pueda accederla en el momento en que necesitan utilizarla.

Este principio está asociado a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de los negocios de la empresa o de las personas, sin impactos negativos para la utilización de las informaciones.

No basta estar disponible: la información deberá estar accesible en forma segura y oportuna para que se pueda usar en el momento en que se solicita y que se garantice su integridad y confidencialidad.

Así, el ambiente tecnológico y los soportes de la información deberán estar funcionando correctamente y en forma segura para que la información almacenada en los mismos y que transita por ellos pueda ser utilizada por sus usuarios.

Garantía de la disponibilidad de la información para que se pueda garantizar la disponibilidad de la información, es necesario conocer cuáles son sus usuarios, con base en el principio de la confidencialidad, para que se puedan organizar y definir las formas de colocación en disponibilidad, garantizando, conforme el caso, su acceso y uso cuando sea necesario.

La disponibilidad de la información se deberá considerar con base en el valor que tiene la información y en el impacto resultante de su falta de disponibilidad.

Para aumentar aún más la disponibilidad de la información deberán:

Definirse estrategias para situaciones de contingencia. Establecerse rutas alternativas para el tránsito de la información, para garantizar su acceso y la continuidad de los negocios incluso cuando algunos de los recursos tecnológicos, o humanos, no estén en perfectas condiciones de operación.

En el mundo actual de cambios rápidos, la necesidad de información oportuna significa a menudo que esté disponible en tiempo real correspondiente a las condiciones del momento. La información completa brinda a los administradores lo que necesitan para ejercer el proceso de control, coordinar o tomar una decisión eficaz.

Ahora bien, los administradores rara vez tienen la información completa; más bien, por obra de la incertidumbre, la ambigüedad y la racionalidad acotada,

tienen que conformarse con información incompleta. Una de las funciones de los sistemas de información es completar la información que se pone a disposición de los administradores.

3. Integra (Información Correcta):

Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada.

Para que la información se pueda utilizar, deberá estar íntegra. Cuando ocurre una alteración no autorizada de la información en un documento, quiere decir que el documento ha perdido su integridad.

La integridad de la información es fundamental para el éxito de la comunicación. El receptor deberá tener la seguridad de que la información obtenida, leída u oída es exactamente la misma que fue colocada a su disposición para una debida finalidad. Si una información sufre alteraciones en su versión original, entonces la misma pierde su integridad, ocasionando errores y fraudes y perjudicando la comunicación y la toma de decisiones.

La quiebra de integridad ocurre cuando la información se corrompe, falsifica o burla.

Una información se podrá alterar de varias formas, tanto su contenido como el ambiente que la soporta. Por lo tanto, la quiebra de la integridad de una información se podrá considerar bajo dos aspectos:

1. Alteraciones del contenido de los documentos donde se realizan inserciones, sustituciones o remociones de partes de su contenido;
2. Alteraciones en los elementos que soportan la información donde se realizan alteraciones en la estructura física y lógica donde una información está almacenada. Citemos unos ejemplos:

Cuando se alteran las configuraciones de un sistema para tener acceso a informaciones restrictas, cuando se superan las barreras de seguridad de una red de computadoras. Por lo tanto, la práctica de la seguridad de la información tiene como objeto impedir que ocurran eventos de quiebra de integridad, causando daños a las personas y empresas.

Garantía de la integridad de la información es asegurarnos que sólo las personas autorizadas puedan hacer alteraciones en la forma y contenido de una información, así como en el ambiente en el cual la misma es almacenada y por el cual transita, es decir, en todos los activos. Por lo tanto, para garantizar la integridad, es necesario que todos los elementos que componen la base de gestión de la información se mantengan en sus condiciones originales definidas por sus responsables y propietarios.

La exactitud y el grado de confiabilidad son factores críticos que determinan la calidad de la información. Cuanto más precisa y confiable sea la información, mayor es su calidad. Para que los SI funcionen bien, la información que provee debe ser de calidad. Si los administradores concluyen que la información que les provee el SI que usan es de mala calidad, le perderán la confianza y dejarán de usarla. Igualmente, si los administradores basan sus decisiones en información de baja calidad, tomarán malas decisiones, e incluso desastrosas.

4. Confidencial (Usuario Autorizado)

Tiene como propósito el asegurar que sólo la persona correcta acceda a la información que queremos distribuir. La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona.

Eso significa que estos datos deberán ser conocidos sólo por un grupo controlado de personas, definido por el responsable de la información. Por ese

motivo, se dice que la información posee un grado de confidencialidad que se deberá preservar para que personas sin autorización no la conozcan.

Pérdida de confidencialidad significa pérdida de secreto. Si una información es confidencial, es secreta, se deberá guardar con seguridad y no ser divulgada para personas no autorizadas.

Garantía de la confidencialidad de la información: involucra a todos los elementos que forman parte de la comunicación de la información, desde su emisor y los dispositivos de entrada, el camino que ella recorre y los dispositivos de comunicación, hasta su receptor dispositivos de salida o almacenamiento.

Y también, cuanto más valiosa es una información, mayor debe ser su grado de confidencialidad. Y cuanto mayor sea el grado de confidencialidad, mayor será el nivel de seguridad necesario de la estructura tecnológica y humana que participa de este proceso: del uso, acceso, tránsito y almacenamiento de las informaciones.

Se deberá considerar a la confidencialidad con base en el valor que la información tiene para la empresa o la persona y los impactos que podría causar su divulgación indebida. Siendo así, debe ser accedida, leída y alterada sólo por aquellos individuos que poseen permisos para tal.

El acceso debe ser considerado con base en el grado de sigilo de las informaciones, pues no todas las informaciones sensibles de la empresa son confidenciales

La forma de instrumentar la confidencialidad de la información es a través del establecimiento del grado de sigilo, veamos enseguida este concepto fundamental:

Grado de sigilo: que es una graduación atribuida a cada tipo de información dependiendo del tipo de información y del público para el cual se desea colocar a

disposición los grados de sigilo podrán ser: Confidencial, Restricto, Sigiloso, Público

5. No Repudio (Aceptación de Creación o Recibo)

Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático. Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales. Se habla entonces de:

- No Repudio de Origen: el emisor no puede asumir que él ha sido quien envió la información.
- No Repudio de Destino: el destinatario no puede asumir que no ha recibido la información.

Cabe mencionar que independientemente de que la información cumpla con las características antes enlistadas, está presente el riesgo en la manipulación de esta, puesto que viaja por medios propiamente “no seguros” como lo son la infraestructura implementada para su manejo, así como los procesos a los cuales es sometida, tanto como por los usuarios que la utilizan.

2.2 EL DATO.

“Es la representación formal de hechos, conceptos o instrucciones adecuada para su comunicación, interpretación y procesamiento por seres humanos o medios automáticos.”[14]

[14] http://elvex.ugr.es/decsai/java/pdf/2C-Datos.pdf

2.2.1 TIPOS DE DATOS.

Debemos considerar que los datos son tratados de distintas formas según su entorno de operación, pues se encuentran dispuestos a los usos y/o aplicaciones que sus administradores requieran, para efectos de nuestro estudio, nos valdremos un enfoque informático, para esto se presenta el siguiente ejemplo de operación:

La especificación de un dominio (rango de valores) y de un conjunto válido de operaciones a los que normalmente los traductores asocian un esquema de representación interna propio se rigen por las siguientes características:

Clasificación de los tipos de datos:

En función de quién los define:

- Tipos de datos estándar
- Tipos de datos definidos por el usuario
- Tipos de datos de aplicación

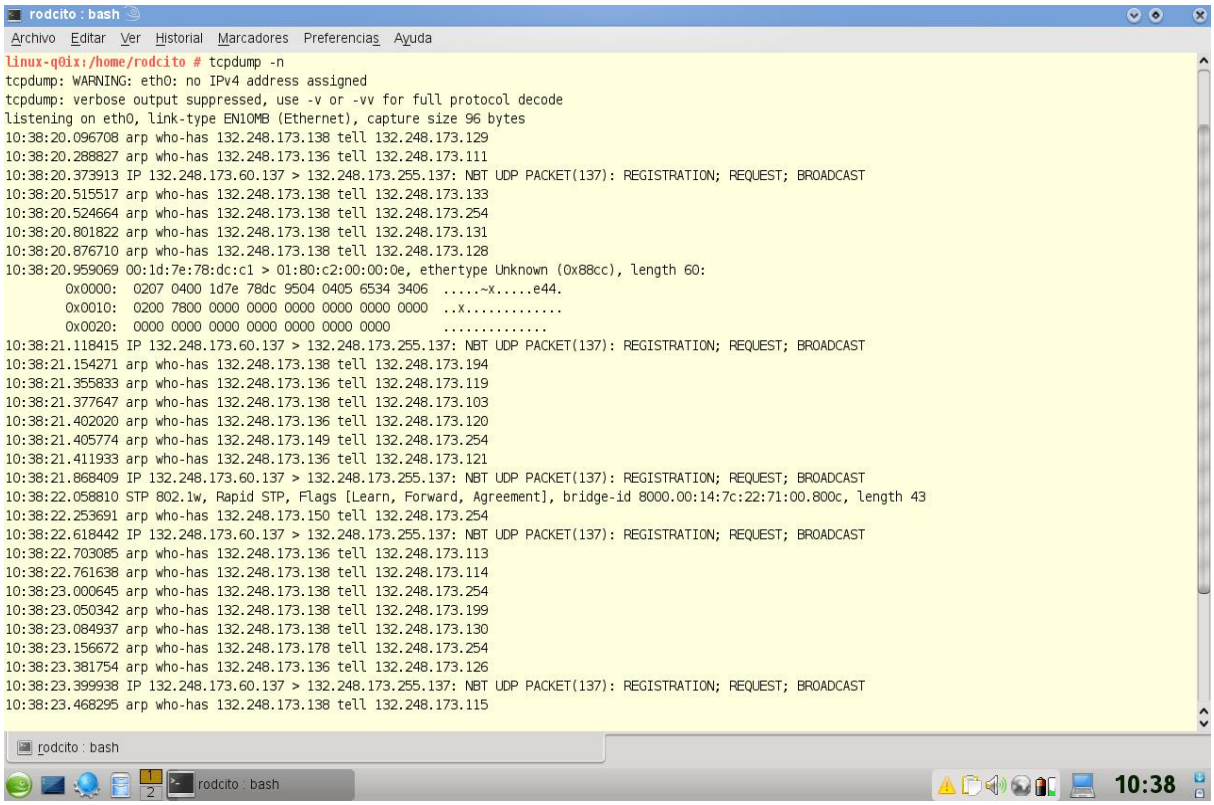
Dada la importancia de los datos de aplicación para nuestra publicación, he aquí unas utilerías para el manejo de estos:

Tcpdump (y su port a Windows, Windump) son programas cuya utilidad principal es analizar el tráfico que circula por la red. Se apoya en la librería de captura pcap, la cual presenta una interfaz uniforme y que esconde las peculiaridades de cada sistema operativo a la hora de capturar tramas de red.

Así mismo, permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual la computadora está conectada. Está escrito por Van Jacobson, Craig Leres, y Steven McCanne que trabajaban en ese momento en el Grupo de Investigación de Red del Laboratorio Lawrence Berkeley. Más tarde el programa fue ampliado por Andrew Tridgell.

Tcpdump funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, tcpdump hace uso de la librería libpcap para capturar los paquetes que circulan por la red.

Existe una adaptación de tcpdump para los sistemas Windows que se llama WinDump y que hace uso de la librería Winpcap.



En UNIX y otros sistemas operativos, es necesario tener los privilegios del root para utilizar tcpdump.

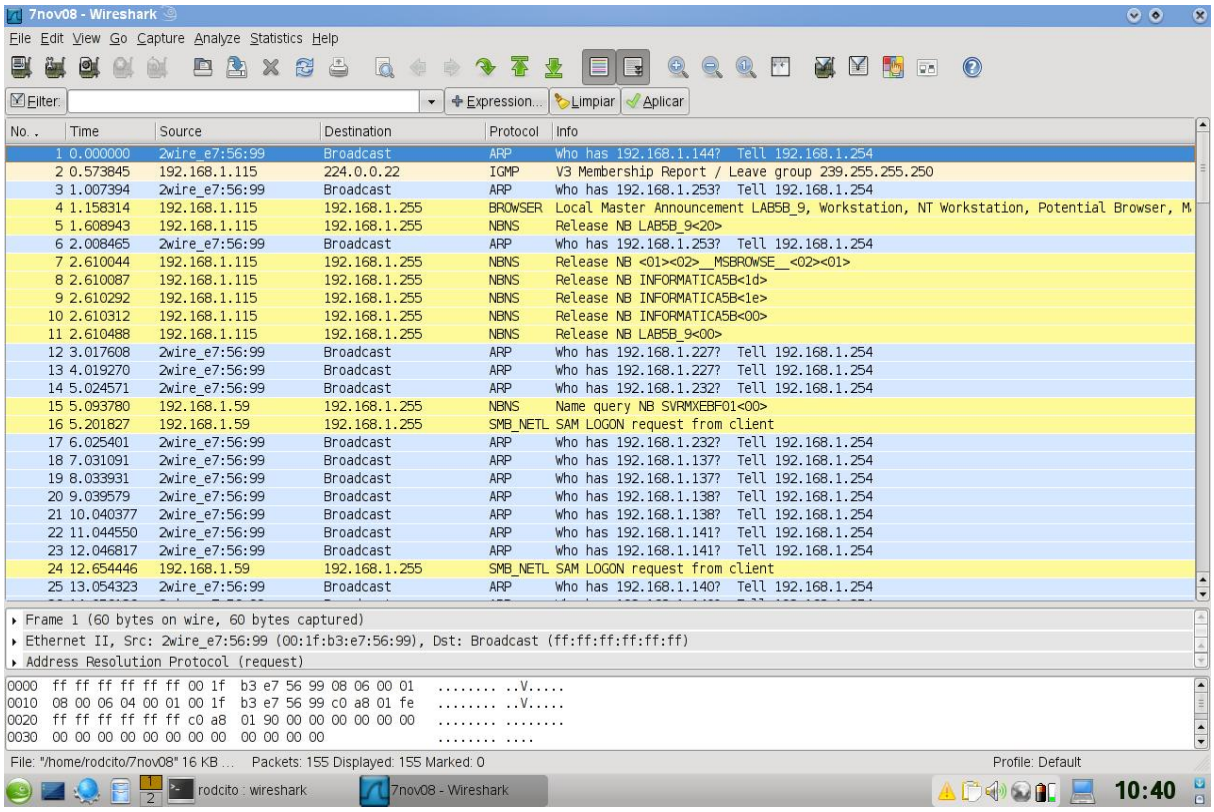
El usuario puede aplicar varios filtros para que sea más depurada la salida. Un filtro es una expresión que va detrás de las opciones y que nos permite seleccionar los paquetes que estamos buscando. En ausencia de ésta, el tcpdump volcará todo el tráfico que vea el adaptador de red seleccionado.

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones

para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

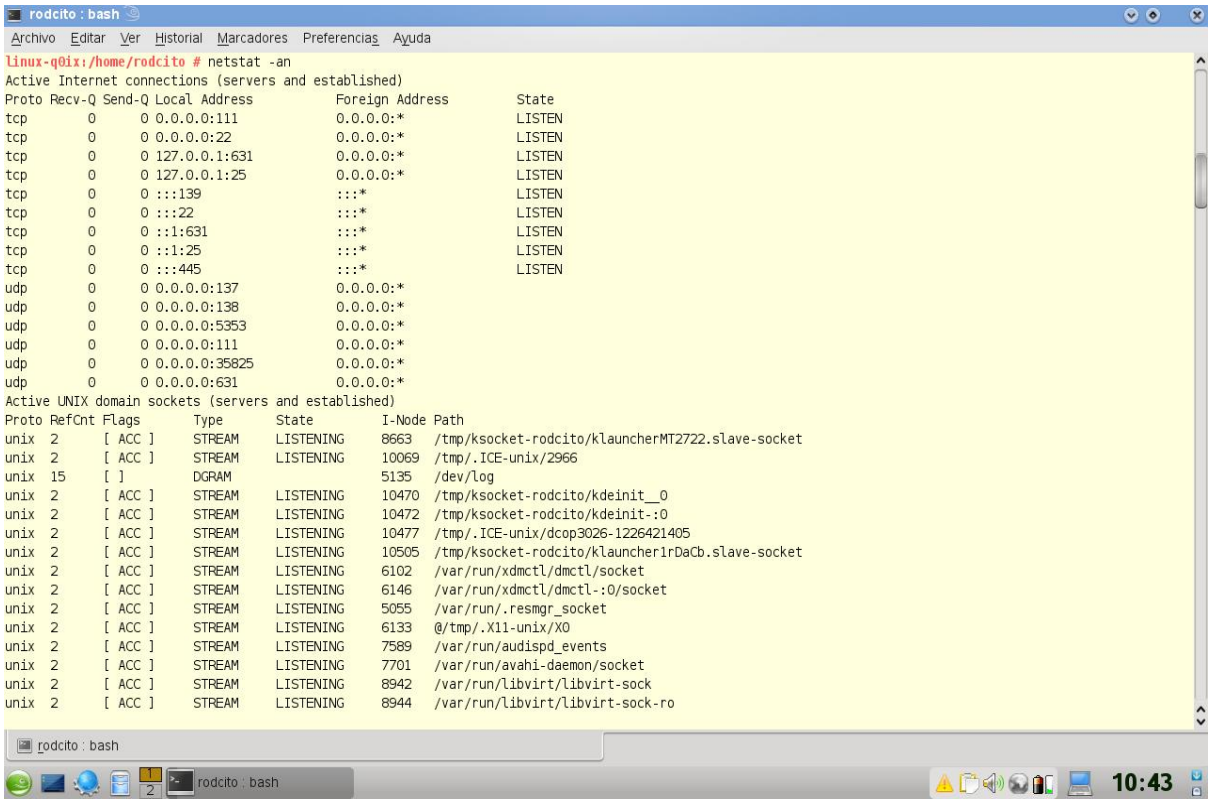
Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.



Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

En función de su representación interna:

- Tipos de datos escalares o simples
- Tipos de datos estructurados



2.2.2 CODIFICACIÒN DE LOS DATOS EN LA COMPUTADORA.

En el interior de la computadora, los datos se representan en binario.

El sistema binario sólo emplea dos símbolos: 0 y 1

⇒ Un bit nos permite representar 2 símbolos diferentes: 0 y 1

⇒ Dos bits nos permiten codificar 4 símbolos: 00, 01, 10 y 11

⇒ Tres bits nos permiten codificar 8 símbolos distintos:

000, 001, 010, 011, 100, 101, 110 y 111

En general, con N bits podemos codificar 2^N valores diferentes, obsérvese la siguiente tabla:

N	2^N
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192
14	16384
15	32768
16	65536

Tabla 2

Si queremos representar X valores diferentes, necesitaremos N bits, donde N es el menor entero mayor o igual que $\log_2 X$.

2.3 SEGURIDAD DE LA INFORMACIÓN.

Dado que es difícil controlar los errores que comenten tanto los administradores de los sistemas de información como los usuarios y a la vez es improbable predecir cuando un disco duro fallará, así mismo; ya que la información y los datos son transmitidos por medios electrónicos poco seguros como lo son las redes de comunicación de datos como LAN´s, WAN´s, MAN´s y VPN´s, por mencionar algunas, por estas razones es primordial contrarrestar estos posibles problemas con la finalidad de proteger toda la información (datos) con que se trabaja diariamente.

En lo siguiente se describen los conceptos básicos con los que trabajan los sistemas informáticos para proteger la información.

2.3.1 CONCEPTOS GENERALES DE LA ENCRIPTACIÓN DE DATOS.

Vamos a presentar en este apartado las nociones esenciales de esta ciencia y los sistemas de encriptación de datos más comunes, necesarios para comprender los actuales estándares de transmisión de datos segura.

Para esto, entendemos por "Criptografía (Kriptos=ocultar, graphos=escritura) la técnica de transformar un mensaje inteligible, denominado texto en claro, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos criptograma o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina algoritmo de encriptación."[15]

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

La base de la Criptografía suele ser la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose criptosistema o sistema de cifrado a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

Criptografía clásica.

El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, sobre todo en el campo militar y en aquellos otros en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros.

[15] Por Luciano Moreno, del departamento de Software de BJS Software

Aunque en cierta forma el sistema de jeroglíficos egipcio puede considerarse ya una forma de criptografía (sólo podían ser entendidos por personas con conocimientos suficientes), el primer sistema criptográfico como tal conocido de debe a Julio Cesar. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino. En nuestro alfabeto actual tendríamos la siguiente tabla de equivalencias:

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

Tabla 3

Por lo que el mensaje "HOLA MUNDO" se transformaría en "KRQD OXPGR". Para volver al mensaje original desde el texto cifrado tan sólo hay que tomar un alfabeto e ir sustituyendo cada letra por la que está tres posiciones antes en el mismo.

Este sistema fue innovador en su época, aunque en realidad es fácil de romper, ya en todo sistema de transposición simple sólo hay un número de variaciones posible igual al de letras que formen el alfabeto (27 en este caso).

Este fue el primer sistema criptográfico conocido, y a partir de él, y a lo largo de las historia, aparecieron otros muchos sistemas, basados en técnicas criptológicas diferentes. Entre ellos caben destacar los sistemas mono alfabéticos (parecidos al de Julio Cesar, pero que transforman cada letra del alfabeto original en la correspondiente de un alfabeto desordenado), el sistema Playfair de Ser Charles Wheastone (1854, sistema mono alfabético de diagramas), los sistemas poli alfabéticos, los de permutación, etc.

Aunque han sido muchos, y no vamos a verlos a fondo, sí hay que destacar los sistemas generales de ocultación, ya que juntos forman la base de muchos de los sistemas criptográficos actuales.

2.3.2 MÉTODOS PARA LA ENCRIPTACIÓN DE DATOS.

Fundamentos matemáticos.

NOTA: Este apartado puede resultar complejo para aquellas personas con un conocimiento limitado de matemáticas, especialmente de Álgebra de conjuntos, Matemática Discreta y Aritmética Modular. No obstante, lo incluimos porque es necesario si se quiere adquirir una base sólida de cómo funcionan y se crean los sistemas de codificación en Criptografía. Procuraré ser lo más somero en conceptos matemáticos puros, usando sólo aquellos necesarios para dar sentido al apartado.

Los sistemas criptográficos modernos, tanto si son de clave simétrica como de llave pública, para ser considerados tales deben cumplir una serie de requisitos que los hagan seguros, reversibles y viables. Para obtener sistemas que cumplan estas condiciones se ha desarrollado un campo matemático completo, la Teoría de Códigos, basado en el álgebra de los sistemas discretos y en las clases residuales de módulo dado, que sirve para definir alfabetos y funciones que permiten obtener sistemas robustos.

Generalmente, todo sistema criptográfico se basa en la obtención de un conjunto de elementos, llamados letras o símbolos, que forman un conjunto finito llamado **alfabeto fuente**, **alfabeto fuente** y en una función de transformación de dichos símbolos en otros pertenecientes a un conjunto imagen denominado **código**. A la función de transformación de le llama **función de codificación**, f_k, y a las sucesiones finitas de elementos del alfabeto fuente se les denominan **palabras**. En general, habrá una función de codificación f_k para cada valor de la clave k, definiendo éstas el **conjunto de claves del sistema**, **K**.

Si consideramos ahora otro conjunto de símbolos A y el conjunto asociado A* de todas las palabras posibles que se pueden formar con las letras de A, se denomina **código C** a todo subconjunto finito de éste. Si C está formado por palabras de longitud fija "n", a n se le llama **longitud del código C**, y a sus

elementos n-palabras. Y si C está formado por "m" elementos, se dice entonces que C es un (n,m) código.

Se define un criptosistema como una quíntupla (M,C,K,E,D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados (criptogramas).
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de las transformaciones de cifrado, es decir, el conjunto de funciones matemáticas que se aplican a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor de la clave k.
- D es el conjunto de transformaciones de descifrado, análogo al conjunto E.

Con esta nomenclatura, todo sistema de cifrado debe cumplir la condición:

$$\mathbf{D_k(E_k(m))=m}$$

Para aclarar un poco estos conceptos, vamos a ver un ejemplo basado en nuestro alfabeto castellano. Este sería el alfabeto fuente, las letras (a, b, c, d, e, ...) serían las letras o símbolos del mismo, y las combinaciones de diferentes letras (casa, perro, silla, ...) serán las palabras del alfabeto. Sólo nota que desde un punto de vista matemático y criptográfico también serán palabras dekid, podretyp, lloeer y cualquier otra formada por cualesquiera de las letras del alfabeto fuente, no siendo necesario que tengan sentido alguno.

Sea A = alfabeto castellano.

Sea S el alfabeto fuente, subconjunto de A, que es esta caso va a ser S = A, es decir, vamos a considerar como alfabeto fuente todo el alfabeto castellano.

Sea C el código C = A = alfabeto castellano.

Definimos nuestra función de codificación, f_1, como: S--f_1-->C, tal que a cada letra le hace corresponder su siguiente en el alfabeto fuente, es decir, la función realizará las siguientes transformaciones, Véase la siguiente tabla:

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

Tabla 4

Consideremos entonces el conjunto M de textos en plano que se pueden formar con las palabras de S, y dentro de él el elemento M_1 = HOLA MUNDO. La función de codificación sería en esta caso $f_1(s)= s+k=s+1$, es decir, la función de cifrado desplaza k posiciones cada letra del alfabeto, siendo en nuestro caso k=1 (k es la clave de cifrado).

Por lo tanto, al aplicar la función f_1 a M_1 tendremos: $f_1(M_1)=f_1$(HOLA MUNDO)=IPMB NVQEP (Figura 4).

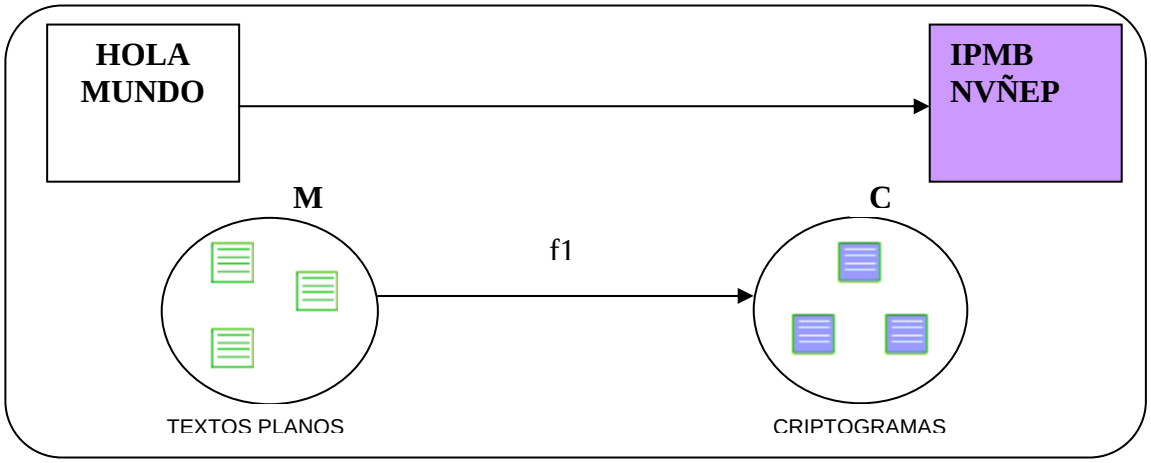


Figura 4

Para que una función pueda ser considerada de codificación debe ser biyectiva, por lo que debe cumplir:

1. elementos diferentes deben tener imágenes diferentes, es decir, no puede haber dos palabras del alfabeto fuente que tengan la misma transformación en el código.
2. todos los elementos deben tener imagen, o lo que es lo mismo, no puede haber palabras del alfabeto fuente que no tengan su transformación en el código.
3. no puede haber palabras del código que no se correspondan con alguna palabra del alfabeto fuente.

Estas tres propiedades se resumen diciendo que f debe ser una aplicación uno a uno.

La exigencia de ser biyectiva se traduce en evitar errores, en que la codificación de un mensaje sea única, y su decodificación también. No obstante, muchos sistemas criptográficos implementan una serie de elementos para la identificación y corrección de errores, ya que durante su viaje por el medio los datos pueden sufrir tales alteraciones que la decodificación resulte incorrecta.

No vamos a extendernos mucho más, pero tenemos que ver otro concepto importante. Normalmente las funciones de codificación reales trabajan con números, ya que es la forma que tiene el computador de operar con rapidez, sobre todo teniendo en cuenta que él pasa los números al sistema binario.

Una función de codificación debe ser tal que con ella obtener las imágenes en el código de los elementos del alfabeto fuente sea un proceso simple y rápido, pero la operación contraria, obtener elementos del alfabeto fuente a partir de sus imágenes en el código, si no se conocen ciertos datos (la clave) debe resultar lo más complicado posible. Ese es el verdadero sentido de una buena función de codificación.

La inclusión de las claves en los procesos de encriptación y desencriptación se realiza introduciendo las mismas en los procesos matemáticos pertinentes, generalmente como constantes en la función de codificación. Cuánto más longitud

tenga la clave usada, más seguro será el sistema de encriptación y más difícil será romperlo por criptoanálisis, aunque esta fortaleza del cifrado también depende del sistema en sí.

Por ejemplo, los sistemas simétricos tienen, a igualdad de longitud de clave, mucha más fortaleza que los de clave pública. Es por esto que los sistemas simétricos usan 58-128 bits generalmente, mientras que los asimétricos deben manejar claves de más de 512 bits para ser considerados seguros.

Un último concepto es el de las clases residuales. Dados dos números enteros, a y b, se dice que **a es congruente con b módulo n** si a y b tienen el mismo resto al ser divididos por n. Por ejemplo, 7 y 10 son congruentes módulo 3, ya que al dividir ambos por 3 nos queda de resto 1.

Con esta consideración, dado un conjunto C se definen sobre él las clases residuales de módulo n como los subconjuntos de C formados por todos sus elementos tales que al ser divididos por n dan el mismo resto.

Por ejemplo, si C = {13,14,15,16,17,18,19} tendremos como clases residuales de módulo 3:

C1 = {15,18} (al dividirlos entre 3 el resto es 0)

C2 = {13,16,19} (al dividirlos entre 3 el resto es 1)

C3 = {14,17} (al dividirlos entre 3 el resto es 2)

Este concepto es importante, ya que muchas de las funciones de codificación usados en los sistemas criptográficos más usados están basadas en las clases residuales del alfabeto fuente.

Para ello manejan la denominada **función módulo discreto**. De esta forma, a mod (b) representa el resto de dividir a entre b. Si a es inferior a b, tendremos que a mod (b)=a. Vamos a ver algunos ejemplos:

17 mod (6)=5 (ya que 17/6=2 con resto 5)

51 mod (6)=3 (ya que 51/6=8 con resto 3)

4 mod (6)=4 (ya que 4<6)

Y tras este apartado un poco dificultoso, vamos a seguir ahora viendo los sistemas criptográficos más usados.

Las técnicas de encriptación suelen dividir a los algoritmos en dos grupos: los algoritmos de clave privada y los algoritmos de clave pública. A los algoritmos de clave privada se los llama también algoritmos de encriptación simétricos mientras que los de clave pública suelen denominarse algoritmos antisimétricos.

Algoritmos de clave simétrica[16]

Los algoritmos de clave simétrica, también llamados de clave secreta o privada, son los algoritmos clásicos de encriptación en los cuales un mensaje es encriptado utilizando para ello una cierta clave, sin la cual no puede recuperarse el mensaje original.

El esquema básico de los algoritmos de clave simétrica es (Figura 5):

MENSAJE + CLAVE = CÓDIGO (encriptación)

CÓDIGO + CLAVE = MENSAJE (desencriptación)

[16] Lomonaco, Samuel J. Jr. A Talk on Quantum Cryptography or How Alice Outwits Eve. 2001.

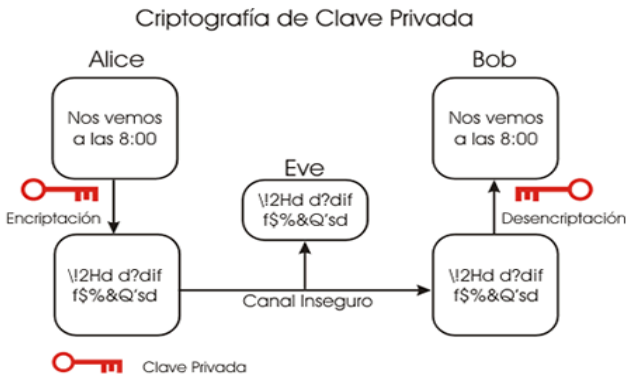


Figura 5

Esto se lleva a cabo sustituyendo porciones del mensaje original por porciones de mensaje encriptado usando la clave. La sustitución puede ser de varias formas:

Monoalfabética:

Cuando se encripta, cada carácter encriptado corresponde a un carácter del mensaje original y viceversa.

Homofónica:

Cuando un carácter de texto original se encripta en varios caracteres del texto encriptado.

Poligráfica:

Cuando n caracteres del mensaje original generan n caracteres del mensaje encriptado.

Polialfabética:

Cuando n caracteres del texto original se encriptan en m caracteres del texto encriptado ($m \neq n$).

Cabe destacar que la sustitución poligráfica y la sustitución homofónica son casos particulares de la sustitución poli alfabética.

Criptosistemas:

Definiremos a un criptosistema como un conjunto de tres elementos:

- Un espacio de mensajes: PT que es la colección de todos los posibles mensajes pt que pretendemos enviar.
- Un espacio de claves K. Cada clave k determina un método de encriptación Ek y un método de desencriptado Dk. De forma tal que Ek(pt) = código y Dk(código)=pt.
- Un espacio de códigos: CT que es la colección de todos los posibles códigos ct.

Sistemas monoalfabéticos y polialfabéticos:

Un algoritmo de encriptación por clave privada es monoalfabético si cada ocurrencia de un mismo carácter en el mensaje original es reemplazada siempre por un mismo carácter en el código cifrado.

Un algoritmo de encriptación por clave privada es polialfabético si cada ocurrencia de un mismo carácter en el mensaje original es reemplazada por distintos caracteres en el código cifrado.

Desarrollaremos a continuación algunos de los criptosistemas de clave privada mas conocidos, desde los más básicos hasta los más complejos.

Modos de operación para encriptación de bloques.

Al utilizar algoritmos de clave privada de, por ejemplo 64 bits de longitud para encriptar textos de más de 64 bits debe considerarse alguna técnica particular, el método mas simple consiste en dividir el bloque a comprimir en porciones de igual longitud que la clave y encriptar cada uno en forma

independiente. Este método se conoce como Electronic Code Block (ECB) pero existen otras técnicas, los modos de operación Standard ANSI/FIPS son:

ECB: Electronic Code Block.

CBC: Cipher Block Chainning.

CFB: Cipher Feedback.

OFB: Output Feedback.

Sobre la forma en que trabaja cada método puede consultarse el Standard ANSI/FIPS correspondiente.

Deficiencias de los algoritmos de clave privada:

Los algoritmos de clave privada pueden construirse tan eficientes como se desee utilizando passwords más y más largos, sin embargo por más largo que sea el password estos algoritmos presentan una vulnerabilidad evidente: el password.

En un esquema de encriptación por clave privada todo aquel que conozca el password es capaz de desencriptar un mensaje, de aquí que a veces, es mas importante estudiar como proteger el password que como trabaja el algoritmo elegido. Además, muchas veces es necesario transmitir, o enviar el password a alguna persona por lo que será necesario a su vez encriptar el password ingresando en un loop infinito.

Muchas veces el password es tan vulnerable que los criptoanalistas no se molestan en descifrar el código interceptado sino que directamente intentan averiguar el password. Uno de los ejemplos más habituales consiste en averiguar passwords que permiten el acceso a determinados sistemas: cuentas bancarias, computadoras, computadoras donde se guardan otros passwords, etc. A continuación mencionamos algunas de las técnicas mas utilizadas para 'robo de passwords'.

Shoulder Surfing.

Esta técnica es la más básica y consiste en merodear a aquellas personas que conocen el password que se quiere averiguar intentando ver si se consigue visualizar el momento en que el password es tipeado en un teclado o escrito en algún papel, variantes más modernas de esta técnica incluyen programas residentes que monitorean las teclas que se oprimen en el teclado, cámaras que registran lo que se tipea desde un punto elevado, etc. La forma mas elemental es como su nombre lo indica observar por encima del hombro de la persona que tipea el password, parece tonto pero se utiliza muchísimo.

Caballos de Troya.

Los caballos de Troya son programas que se diseñan con el fin específico de robar passwords. El programa es introducido en una computadora y lo que hace es simplemente cada vez que es ejecutado pedirle el password al usuario y si este lo tipea (grave error) guardarlo en un archivo. Luego lo único que hay que hacer es cada tanto consultar el archivo y ver que es lo que nuestro caballo de Troya ha 'pescado'. Una de las reglas de seguridad mas importantes que establecen los administradores de sistemas es adiestrar a los usuarios para que **JAMAS** ingresen su password una vez que se han logoneado en el sistema, además suele ser recomendable resetear la terminal antes de logonearse al sistema por si el usuario anterior dejo andando un caballo de Troya que imita al programa de login.

Ingeniería Social.

Esta disciplina puede parecer ridícula pero es la más exitosa en cuanto a robo de passwords. La Ingeniería Social consiste en conseguir que una persona, simplemente, le diga su password a otra. Las técnicas son de lo mas variadas: llamados telefónicos pidiendo el password pues se cayó un disco y hay que backupear la información de cada usuario, pedidos de password para

'verificaciones rutinarias', encuestas a ver quien tiene el password mas seguro (!!!!), etc, etc...

Aunque parezca mentira hay personas realmente especializadas en este tipo de ataques.

La importancia del mensaje.

Contrariamente a lo que se cree habitualmente, la fuerza de un criptosistema de clave privada no reside únicamente en el algoritmo utilizado, o en la longitud de la clave sino que depende, también, del mensaje a enviar. Hay mensajes que por sus características propias serán mas fáciles de descifrar que otros, dado un mismo criptosistema, por lo tanto a la hora de enviar un texto ultra-secreto debemos tener en cuenta varios factores relacionados con el mensaje en sí.

Recomendaciones a la hora de escribir un texto altamente critico que deba ser encriptado por clave privada:

- No utilizar espacios en blanco, escribir todo el texto de corrido. Cualquier carácter de alta probabilidad de ocurrencia, como por ejemplo los espacios en blanco, son un punto débil en el mensaje aun cuando se utilice un esquema poli alfabético.
- Si es muy necesario separar las palabras del mensaje a enviar, utilizar cualquier carácter elegido arbitrariamente en reemplazo del espacio en blanco.
- Escribir con mucho cuidado el texto intentando que la distribución de cada carácter utilizado en el texto sea lo mas pareja posible, esto es de gran importancia, evitar el uso de uno o mas caracteres en forma predominante, usar palabras sinónimos, o incluir faltas de ortografía y sintaxis si es necesario. Escribir por ejemplo 'salujdhos pedfdro' que puede ser entendido

fácilmente cuando se descifra el código pero podría llegar a complicar sensiblemente el criptoanálisis.

- Empezar algunas palabras con caracteres que no tengan sentido alguno como por ejemplo la llave que cierra '}' o un punto y coma ';', esto puede desalentar varios intentos criptoanalíticos correctamente orientados.
- Escribir algunas palabras al revés o con todas las vocales al final y las consonantes al principio, una especie de doble codificación.

Por ejemplo: 'sldsauo qrdueio pdreo' quiere decir 'saludos querido pedro'.

Los criptoanalistas que consideren como factor cierto la alternancia de vocales y consonantes en un texto tendrán problemas para descifrar nuestro mensaje. En algunas palabras se pueden poner todas las vocales al final y en otras todas al principio.

- Jamás utilizar dos veces la misma palabra en un texto, aun en sistemas poli alfabéticos esto constituye una debilidad.
- Escribir todos los mensajes de la forma más breve que sea posible, evitar el uso de artículos salvo que sean estrictamente necesarios para comprender el texto. Las claves de éxito de un buen criptoanálisis aumentan vertiginosamente a medida que se consigue más información sobre el mensaje a descifrar.

Criptosistema Caesar.

El sistema Caesar o desplazamientos Caesar es una de las técnicas de criptografía más simples y mayormente difundidas. Fue el primero que se utilizó del cual se tienen registros. El sistema es mono alfabético y es realmente muy malo, su único valor es el valor histórico de haber sido el primero.

En un sistema Caesar la encriptación se hace por sustitución, cada carácter del mensaje original será reemplazado por un carácter en el mensaje cifrado, el

carácter cifrado se obtiene avanzando 'k' pasos en el alfabeto a partir del carácter original. Obviamente 'k' es la clave.

Ejemplo con **k=2**:

Si el texto original es "ABCDE" se codifica como "CDEFG", analice la siguiente figura:

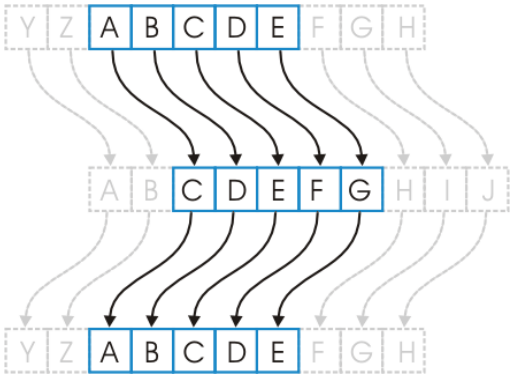


Figura 6

Este es todo el secreto del sistema 'CAESAR' veamos ahora cuan malo es:

Criptoanálisis.

Para el sistema Caesar la tarea de un criptoanalista es realmente sencilla, pues la cantidad de posibles claves de este sistema es muy limitada. Trabajando con un alfabeto de 25 caracteres hay solamente 25 posibles claves (1..25) la clave 26, es idéntica a la clave 1, la clave 27 es idéntica a la 2 y así sucesivamente. De esta forma el criptoanalista puede chequear una por una las 25 posibles claves y observando el resultado obtenido se llega fácilmente y en muy poco tiempo al mensaje original.

Este es un criptosistema cuyo punto débil es el espacio de claves, como hay muy pocas claves posibles la técnica mas recomendable para el criptoanalista es simplemente probar todas las posibles claves. A este método se lo denomina

'ataque por fuerza bruta' y cuando el tiempo estimado para el ataque es razonable es un método infalible.

Criptosistema Hill.

Este sistema esta basado en el álgebra lineal y ha sido importante en la historia de la criptografía. Fue Inventado por Lester S. Hill en 1929, y fue el primer sistema criptográfico poli alfabético que era práctico para trabajar con más de tres símbolos simultáneamente.

Este sistema es poli alfabético pues puede darse que un mismo carácter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado.

Suponiendo que trabajamos con un alfabeto de 26 caracteres.

Las letras se numeran en orden alfabético de forma tal que A=0, B=1, ... ,Z=25 (Tabla 5).

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

Tabla 5

Se elije un entero d que determina bloques de d elementos que son tratados como un vector de d dimensiones.

Se elije de forma aleatoria una matriz de d × d elementos los cuales serán la clave a utilizar.

Los elementos de la matriz de d × d serán enteros entre 0 y 25, además la matriz M debe ser invertible en $\mathbb{Z}_{26}^{n}$.

Para la encriptación, el texto es dividido en bloques de d elementos los cuales se multiplican por la matriz d × d

Todas las operaciones aritméticas se realizan en la forma modulo 26, es decir que 26=0, 27=1, 28=2 etc.

Dado un mensaje a encriptar debemos tomar bloques del mensaje de "d" caracteres y aplicar:

$M \times P_i = C$, donde C es el código cifrado para el mensaje P_i

Ejemplo:

Si tomamos la matriz $A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$ como matriz de claves.

Para encriptar el mensaje "CÓDIGO" debemos encriptar los seis caracteres de "CÓDIGO" en bloques de 3 caracteres cada uno, el primer bloque

$$P_1 = \text{"COD"} = \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} \qquad P_2 = \text{"IGO"} = \begin{pmatrix} 6 \\ 8 \\ 14 \end{pmatrix}$$

$$A \cdot P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 308 \\ 349 \\ 197 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix} (\text{mod } 26)$$

El primer bloque "COD" se codificara como "WLP"

$$A \cdot P_2 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 8 \\ 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 422 \\ 252 \\ 264 \end{pmatrix} = \begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix} (\text{mod } 26)$$

El segundo bloque "IGO" se codificara como "GSE"

Luego 'CÓDIGO' encriptado equivale a 'WLPGSE'.

Observar que las dos "O" se codificaran de forma diferente.

Para desencriptar el método es idéntico al anterior pero usando la matriz inversa de la usada para encriptar.

Cálculo de la matriz inversa.

Antes que nada debemos verificar que la matriz elegida sea invertible en modulo 26. Hay una forma relativamente sencilla de averiguar esto a través del cálculo del determinante. Si el determinante de la matriz es 0 o tiene factores comunes con el módulo (en el caso de 26 los factores son 2 y 13), entonces la matriz no puede utilizarse. Al ser 2 uno de los factores de 26 muchas matrices no podrán utilizarse (no servirán todas en las que su determinante sea 0, un múltiplo de 2 o un múltiplo de 13).

Para ver si es invertible calculo el determinante de A

$$\begin{vmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{vmatrix}$$

$5\,(23 \cdot 13 - 3 \cdot 11) - 17\,(9 \cdot 13 - 3 \cdot 2) + 20\,(9 \cdot 11 - 23 \cdot 2) = 1215 - 1734 + 1060 = 503$

$503 = 9 \bmod 26$

La matriz A es invertible en modulo 26 ya que 26 y 9 son co-primos

Para hallar la inversa de la matriz modulo 26, utilizamos la formula

$$A^{-1}=C^{T}\cdot\left(\det(A)\right)^{-1}$$

Donde CT es la matriz de cofactores de A transpuesta

Hay que tener en cuenta que $\left(\det(A)\right)^{-1}$ debe realizarse en modulo 26

por lo tanto para el ejemplo la inversa de 9 (mod 26) es 3 (mod 26) ya que

9 (mod 26) · 3 (mod 26) = 27 mod 26 = 1 (mod 26)

Por lo tanto 3 es la inversa multiplicativa de 9 en modulo 26

Para calcular C hay que calcular los cofactores de A

$$C_{11}=+\begin{vmatrix}23 & 3\\ 11 & 13\end{vmatrix} \qquad C_{12}=-\begin{vmatrix}9 & 3\\ 2 & 13\end{vmatrix} \qquad C_{13}=+\begin{vmatrix}9 & 23\\ 2 & 11\end{vmatrix}$$

$$C_{21}=-\begin{vmatrix}17 & 20\\ 11 & 13\end{vmatrix} \qquad C_{22}=+\begin{vmatrix}5 & 20\\ 2 & 13\end{vmatrix} \qquad C_{23}=-\begin{vmatrix}5 & 17\\ 2 & 11\end{vmatrix}$$

$$C_{31}=+\begin{vmatrix}17 & 20\\ 23 & 3\end{vmatrix} \qquad C_{23}=-\begin{vmatrix}5 & 20\\ 9 & 3\end{vmatrix} \qquad C_{33}=+\begin{vmatrix}5 & 17\\ 9 & 23\end{vmatrix}$$

$$C=\begin{pmatrix}266 & -111 & 53\\ -1 & 25 & -21\\ -409 & 165 & -38\end{pmatrix} \qquad C^{T}=\begin{pmatrix}266 & -1 & -409\\ -111 & 25 & 165\\ 53 & -21 & -38\end{pmatrix}$$

Ahora aplicamos la formula de la inversa

$$A^{-1}=C^{T}\cdot\left(\det(A)\right)^{-1}=\begin{pmatrix}266 & -1 & -409\\ -111 & 25 & 165\\ 53 & -21 & -38\end{pmatrix}\cdot 3$$

$$A^{-1} = \begin{pmatrix} 798 & -3 & -1227 \\ -333 & 75 & 495 \\ 159 & -63 & -114 \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} (\mathrm{mod}\, 26)$$

Esta última es la matriz que utilizamos para desencriptar

Criptoanálisis.

El sistema de Hill plantea a los criptoanalistas problemas mucho mayores a los que planteaba 'CAESAR'. Para empezar el espacio de claves es mucho mayor, en este caso es de 4C25, es decir las permutaciones de 4 elementos tomados de entre 25 posibles. Y usando una matriz más grande la cantidad de posibles claves se puede hacer tan grande como sea necesario para hacer que sea imposible un ataque por fuerza bruta.

Lo mejor que puede hacer un criptoanalista es tratar de conseguir un código para el cual se conozca una parte del mensaje. Y ver si con ambos datos es capaz de encontrar cual fue la matriz utilizada para encriptar el mensaje.

Criptosistema Afines.

El Criptosistema Afin es una clase de encriptación por sustitución y es monoalfabético y simétrico.

Un criptosistema Afín es determinado por dos enteros *a* y *b* siendo

- $a \geq 0$
- $b \leq m$
- *m* es el tamaño del alfabeto.
- Además *a* y *m* deben ser co-primos.

Para encriptar un mensaje a cada carácter se le aplica la siguiente fórmula:

$e(x) = a\,x + b \pmod{m}$

Por ejemplo si:

a=3, *b*=5 y *m*=26

El mensaje que queremos encriptar es "hola".

Toda la aritmética debe ser realizada modulo *m* en este caso 26.

Las letras se numeran en orden alfabético de forma tal que A=0, B=1, ... ,Z=25 (Tabla 6).

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

Tabla 6

La función de encriptación que utilizaremos será:

$$e(x) = 3x + 5 \pmod{26}$$

h=7 => $e(7) = 7 * 3 + 5 = 26 \bmod 26 = 0 = a$

o=14 => $e(14) = 14 * 3 + 5 = 47 \bmod 26 = 21 = v$

l=11 => $e(11) = 11 * 3 + 5 = 38 \bmod 26 = 12 = m$

a=0 => $e(0) = 0 * 3 + 5 = 5 = f$

El mensaje "hola" encriptado es "avmf"

Este es un sistema mono alfabético pues cualquier ocurrencia de un determinado carácter será reemplazado siempre por un único carácter en el mensaje cifrado ya que $e(x) = ax + b$ es función.

El requerimiento de que *a* y *m* sean co-primos asegura que la función $e(x) = ax + b$ sea inyectiva ya que si la función no fuera inyectiva un cierto carácter en el mensaje cifrado podría corresponder a mas de un carácter en el mensaje original y no podríamos descifrar el mensaje.

Dos números 'a' y 'b' son co-primos si su Máximo común divisor es 1. El concepto de números co-primos es de gran importancia en el mundo de la criptografía, este y otros conceptos de la teoría de números son utilizados muy a menudo para encriptar y desencriptar información.

En nuestro ejemplo '3' y '26' son co-primos mientras que '10' y '26' no lo son (MCD=2).

La función de desencriptación es $d(x) = a^{-1}(x - b) \pmod{m}$ donde a^{-1} es la inversa multiplicativa de *a* modulo *m* en el caso de $a = 3$, $a^{-1} = 9$ ya que $3 \cdot 9 = 27 = 1$ modulo 26, por lo tanto la función de desencriptación será:

$$d(x) = 9(x - 5) \pmod{26}$$

Criptoanálisis.

Un criptosistema Afín también es vulnerable a un ataque por fuerza bruta, ya que existen 12 posibles valores para a: 1,3,5,7,9,15,17,19,21,23,25 y 26 posibles valores para b (0..25) de esta forma la cantidad de claves posibles es 12*26=312 pero se debe eliminar el caso (a=1,b=0) pues no encripta, luego la cantidad de posibles claves es 311 y el sistema es completamente vulnerable a un ataque por fuerza bruta.

Criptosistema Playfair.

Este sistema criptográfico fue inventado en 1854 por Charles Wheatstone, pero debe su nombre al Baron Playfair de St Andrews quien promovió el uso de este criptosistema.

El algoritmo utiliza una tabla o matriz de 5x5. La tabla se llena con una palabra o frase secreta descartando las letras repetidas. Se rellenan los espacios de la tabla con las letras del alfabeto en orden. Usualmente se omite la "W" y se utiliza la "V" en su lugar o se reemplazan las "J" por "I". Esto se hace debido a que la tabla tiene 25 espacios y el alfabeto tiene 26 símbolos.

La frase secreta usualmente se ingresa a la tabla de izquierda a derecha y arriba hacia abajo o en forma de espiral, pero puede utilizarse algún otro patrón. La frase secreta junto con las convenciones para llenar la tabla de 5x5 constituye la clave de encriptación.

Por ejemplo:

Si la frase secreta es "CRIPTOSISTEMA PLAYFAIR"

Llenaremos de izquierda a derecha y arriba hacia abajo y omitiremos la W en la siguiente tabla (7).

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

Tabla 7

La encriptación se realiza de la siguiente forma:

El mensaje original que se desea encriptar es dividido en bloques de dos caracteres cada uno y se le aplican las siguientes cuatro reglas en orden

Si en el bloque las dos letras son la misma, se reemplaza la segunda generalmente por una X (o alguna letra poco frecuente) y se encripta el nuevo par.

Si las dos letras del bloque aparecen en la misma fila de la tabla, cada una se reemplaza por la letra adyacente que se encuentra a su derecha (si es la letra que se encuentra en la última posición a la derecha de la fila se la reemplaza con la primera de la izquierda de esa fila). Ej. SM se reemplazará por EA y AE por OM.

Si las dos letras del bloque aparecen en la misma columna de la tabla, cada una se reemplaza por la letra adyacente que se encuentra por debajo (si es la letra que se encuentra en la última posición inferior de la columna se la reemplaza con la primera de arriba de esa columna). Ej. LC se reemplazará por GO y GQ por QC.

Si las letras no se encuentran en la misma fila ni columna se las reemplaza se determina el rectángulo formado por los dos caracteres y se encripta tomando los caracteres que están en las esquinas del rectángulo y en la misma fila que el carácter a encriptar. Ej. SB se reemplazará por MY y KR por HP en la siguiente tabla (8).

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

Tabla 8

Para desencriptar se aplican estas cuatro reglas en forma inversa, descartando las "X" que no tengan sentido en el mensaje final.

Ejemplo:

Si queremos codificar "LENGUAJE"

1. Tomamos "LE" como no están ni en la misma fila ni columna se utiliza la regla 4, "LE" se reemplaza por "FO".

2. Tomamos "NG" como están en la misma fila utilizamos la regla 2, "NG" se reemplaza por "GH".

3. Luego, tomamos "UA" como no están ni en la misma fila ni columna se utiliza la regla 4, "UA" se reemplaza por "ZS".

4. Finalmente tomamos "JE" como están en la misma columna utilizamos la regla 3, "JE" se reemplaza por "VF".

Por lo tanto "LENGUAJE se encriptará como ""FOGHZSVF"

De este esquema podemos deducir que el sistema es poli alfabético pues por ejemplo "LE"="FO" implica que "E"="O" y "JE"="VF" implica que "E"="F" lo cual demuestra que el sistema es poli alfabético. En el sistema Playfair si bien no es cierto que todo carácter siempre sea encriptado en un mismo carácter si vale que todo par de caracteres siempre sea encriptado en el mismo par de caracteres, por lo que en lugar de decir que el sistema es poli alfabético podemos decir que es mono alfabético de orden 2.

Criptoanálisis.

El sistema Playfair es un sistema de encriptación bastante bueno, la cantidad de posibles claves es enorme ya que son las permutaciones de 25 elementos tomados de entre 26 lo cual da un número muy grande como para derrotar al algoritmo por fuerza bruta. Además es un sistema poli alfabético por lo que un análisis de la frecuencia de aparición de cada carácter en el código cifrado no nos aporta nada.

La técnica que se debe utilizar con el esquema Playfair consiste en analizar la frecuencia de aparición de los pares de letras (diagramas) y compararlas con los diagramas mas frecuentes del idioma en el cual se supone que se escribió el mensaje original, en castellano los diagramas más probables son:

Ordenados por frecuencia:

ES,EN,EL,DE,LA,OS,AR,UE,RA,RE,ER,AS,ON,ST,AD,AL,OR,TA,CO

El criptoanalista deberá analizar cual es el diagrama mas ocurrente en el código cifrado y ver que ocurre si se lo reemplaza por 'ES', de esta forma se van probando distintas combinaciones entre los diagramas mas frecuentes en el mensaje cifrado y los diagramas mas frecuentes del idioma hasta que se consigue descifrar el texto. Esta es una técnica muy habitual del criptoanálisis y suele funcionar muy bien.

Los sistemas mono alfabéticos de orden 'N' son vulnerables a este tipo de ataque, en general todo criptoanalista esta preparado con programas específicos para analizar las frecuencias de aparición de caracteres individuales, diagramas, tetragramas, y compararlas con las frecuencias estadísticas de un determinado idioma, los programas se encargan también de generar las pruebas necesarias y todo lo que tiene que hacer el criptoanalista es analizar si el texto que resulta de las pruebas tiene sentido. Incluso esto puede hacerlo el programa comparando el texto contra un diccionario.

Criptosistema Diffie-Hellman.

Este algoritmo de encriptación de Whitfield Diffie y Martin Hellman supuso una verdadera revolución en el campo de la criptografía, ya que fue el punto de partida para los sistemas asimétricos, basados en dos claves diferentes, la pública y la privada. Vio la luz en 1976, surgiendo como ilustración del artículo "New directions in Cryptography".

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos, ya que en la práctica sólo es válido para el intercambio de claves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer) y VPN (Virtual Private Network).

Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número como $Y = X^a \bmod q$. Si bien el cálculo de potencias discretas es fácil, la obtención de su función inversa, el logaritmo discreto, no tiene una solución analítica para números grandes.

Para implementar el sistema re realizan los siguientes pasos (Véase la Figura 7):

1. Se busca un número primo muy grande, **q**.
2. Se obtiene el número _, raíz primitiva de q, es decir, que cumple que _ mod q, $_^2 \bmod q$,...., $_^{q-1} \bmod q$ son números diferentes.
3. _ y q son las claves públicas.

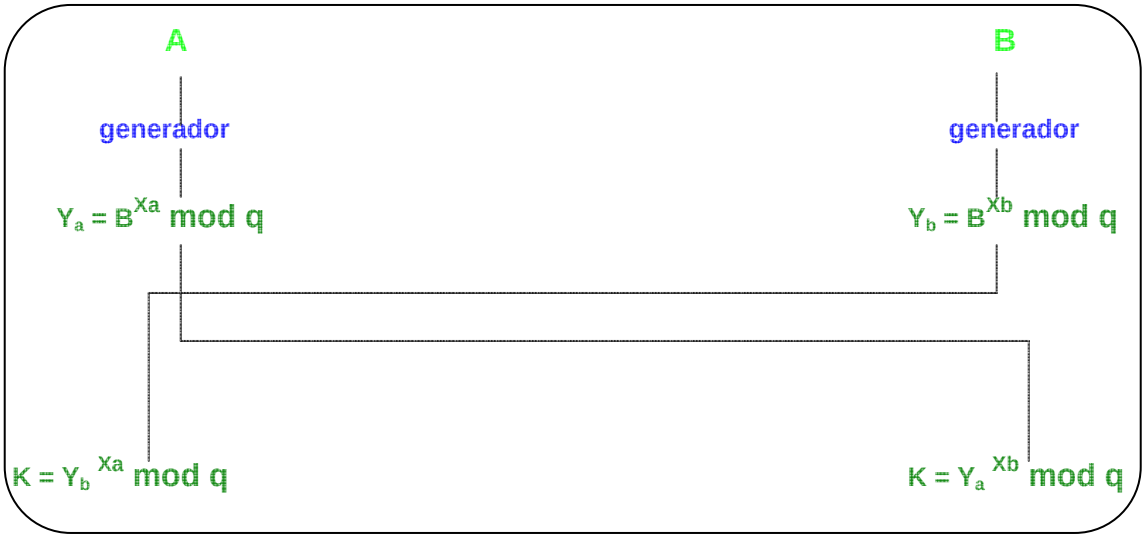


Figura 7: Diffie-Hellman

Para generar una clave simétrica compartida entre dos usuarios, A y B, ambos parten de un generador de números pseudoaleatorios, que suministra un número de este tipo diferente a cada uno, X_a y X_b. Estos son las claves privadas de A y B. Con estos números y las claves públicas _ y q que ambos conocen, cada uno genera un número intermedio, Y_a e Y_b, mediante las fórmulas:

$Y_a = _^{Xa} \bmod q$

$Y_b = _^{Xb} \bmod q$

Estos números son intercambiados entre ambos, y luego cada uno opera con el que recibe del otro, obteniendo en el proceso el mismo número ambos:

$K = Y_b^{Xa} \bmod q$

$K = Y_a^{Xb} \bmod q$

Este número K es la clave simétrica que a partir de ese momento ambos comparten, y que pueden usar para establecer una comunicación cifrada mediante cualquiera de los sistemas simétricos.

Con este esquema, si se desea compartir una clave privada con otro usuario cualquiera, basta con acceder a su Y_u y enviarle la nuestra. Para facilitar este proceso se suelen publicar las Y_u de todos los usuarios interesados en un directorio de acceso común.

Criptosistema IDEA.

Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva y suma y multiplicación de enteros.

El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

Criptosistema RC5.

El sistema criptográfico simétrico RC5 es el sucesor de RC4, frente al que presenta numerosas mejoras. RC4 consiste en hacer un XOR al mensaje con una arreglo que se supone aleatorio y que se desprende de la clave, mientras que RC5 usa otra operación, llamada dependencia de datos, que aplica sifths a los datos para obtener así el mensaje cifrado. Ambos han sido creados por RSA Data Security Inc., la empresa creada por los autores del sistema RSA, que es actualmente una de las más importantes en el campo de los sistemas de cifrado y protección de datos.

Permite diferentes longitudes de clave (aunque está prohibida su exportación fuera de EEUU con longitudes superiores a 56 bits), y funciona como un generador de números aleatorios que se suman al texto mediante una operación de tipo OR-Exclusiva.

Es además ampliamente configurable, permitiendo fijar diferentes longitudes de clave, número de iteraciones y tamaño de los bloques a cifrar, por lo que le permite adaptarse a cualquier aplicación. Por ejemplo, este algoritmo es el usado por Nestcape para implementar su sistema de seguridad en comunicaciones SSL (Secure Socket Layer).

En cuanto a su seguridad, aún es pronto para afirmar nada concluyente, aunque en 1996 una universidad francesa consiguió romper el sistema RC4 con clave de 40 bits, lo que hace sospechar que RC5 con longitudes de clave de 56 bits no es lo suficientemente seguro.

Criptosistema RSA.

El algoritmo de clave pública RSA fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Estos señores se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que

es actualmente una de las más prestigiosas en el entorno de la protección de datos.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Ahora bien, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,... Hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

1. Se buscan dos números primos lo suficientemente grandes: **p** y **q** (de entre 100 y 300 dígitos).
2. Se obtienen los números **n** = p * q y **X** = (p-1) * (q-1).
3. Se busca un número **e** tal que no tenga múltiplos comunes con X.
4. Se calcula **d** = e^{-1} mod X, con mod = resto de la división de números enteros.

Y ya con estos números obtenidos, **n es la clave pública y d es la clave privada**. Los números p, q y X se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 computadoras trabajando juntos para hacerlo).

RSA basa su seguridad es ser una función computacionalmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo X no es factible a menos que se conozca la factorización de e, clave privada del sistema.

RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

Criptosistema PGP.

El sistema PGP (Pretty Good Privacity - Intimidad Bastante Buena) fue diseñado especialmente por Philip Zimmermann en 1991 para proporcionar una forma segura de intercambio de correo electrónico.

Implementa tanto el cifrado del correo y ficheros como la firma digital de documentos. Para la encriptación del documento usa una algoritmo de llave simétrica, con intercambio de clave mediante sistema de llave pública, normalmente RSA, y para la firma digital suele utilizar la función hash MD5. No obstante, es un sistema ampliamente configurable, que permite al usuario elegir entre diferentes sistemas asimétricos, funciones hash y longitudes de clave.

Para usarlo hay que comenzar generando un par de claves, una pública y otra privada, siendo posible en ese momento la elección de la longitud de clave deseada. También hay que fijar una clave personal, que se usará luego para

proteger la llave privada de miradas indiscretas. Las claves pública y privada las genera automáticamente el algoritmo, mientras que la personal de protección la elige el usuario.

Una vez generadas las claves, la privada se encripta con la personal mediante un algoritmo simétrico, siendo posteriormente necesario desencriptarla cada vez que deseemos usarla.

En cuanto a la clave pública, se deposita en un fichero especial, de tipo ASCII (sólo texto), denominado **certificado de clave**, que incluye el identificador de usuario del propietario (el nombre de esa persona y algún dato único, como su dirección de e-mail), un sello de hora del momento en el que se generó el par de llaves y el material propio de la clave.

Cuando se desea mandar un correo o fichero encriptado, PGP lo encripta usando un sistema simétrico, generalmente IDEA o DES, usando una clave aleatoria, que posteriormente se encripta con RSA. Se envían el documento cifrado con la clave aleatoria y ésta encriptada con la llave RSA privada del destinatario.

Cuando éste recibe el correo y desea desencriptarlo, su programa PGP primero descifra la clave simétrica con su llave privada RSA, y luego descifra el documento usando la clave desencriptada. El proceso se ilustra en la siguiente figura (8).

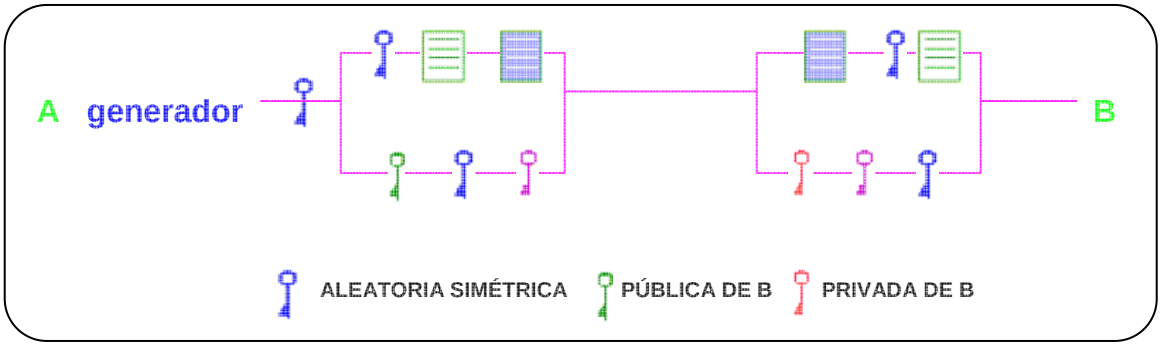


Figura 8: PGP

Normalmente el sistema PGP viene implementado mediante alguna aplicación específica, que se instala en el computador del usuario. Esta aplicación se integra perfectamente con los programas de correo más comunes, permitiendo al usuario el uso directo del sistema PGP, con tan sólo pulsar los botones que aparecerán en la barra de menús de la aplicación de correo.

Para desencriptar un mensaje basta con seleccionar el icono correspondiente (o mediante el botón derecho del ratón), siendo necesario en ese momento introducir la clave personal, para que el programa pueda acceder a la clave pública encriptada. Para firmar un correo se procede de forma análoga.

En el caso de querer enviar un e-mail encriptado a otra persona, es necesario en primer lugar que la misma tenga un programa PGP instalado, y después que nosotros tengamos la llave pública del destinatario. Si es así, basta con seleccionar la opción correspondiente en el menú, con lo que se nos pedirá la clave pública del destinatario, y el programa se encargará de todo lo demás.

Si tenemos la necesidad de cifrar mensajes para muchos destinatarios diferentes nos encontraremos con el problema de gestionar los distintos ficheros de llave pública. Para ello, los programas PGP facilitan el denominado **llavero**, que es un pequeño módulo de software que se encarga de administrar dichos ficheros. Cuando recibamos uno de ellos, basta con colocarlo en el llavero para tenerlo disponible siempre que deseemos.

Puede interesarnos en un momento dado enviar un correo cifrado o vernos en la necesidad de comprobar la autenticidad de un correo que nos llega firmado por parte de un destinatario del que no conocemos su llave pública.

Podemos obtener ésta dirigiéndonos directamente a dicha persona y pidiéndosela, pero para facilitar esta tarea, y puesto que el objeto de las llaves públicas es ser difundidas lo más posible, se han habilitado diferentes servidores que poseen bases de datos con las claves públicas de los usuarios de PGP. Basta

acudir a los mismos y solicitar el fichero de clave correspondiente a la persona que nos interesa.

El uso de RSA ha hecho que la difusión y uso de PGP se haya visto sujeta a las controversias provocadas por la necesidad de una licencia de exportación, lo que le ha costado a Phill Zimmermann ser procesado por ello.

Criptosistema DES.

Finalmente analizaremos el sistema de encriptación por clave privada mas difundido y ampliamente utilizado en el mundo conocido como 'DES' (Data encription estándar) Cuando fue creado el algoritmo se suponía tan fuerte que inmediatamente se propuso como estándar y se dio a conocer el algoritmo.

El Estándar Federal para encriptación de datos. (DES) fue durante mucho tiempo un buen algoritmo de encriptación para la mayoría de las aplicaciones comerciales. El gobierno de USA, sin embargo nunca confío en el DES para proteger sus datos clasificados debido a que la longitud de la clave del DES era de solamente 56 bits, lo suficientemente corta como para ser vulnerable a un ataque por fuerza bruta.

El ataque mas devastador contra el DES fue descripto en la conferencia Crypto'93 donde Michael Wiener de Bell presento un trabajo sobre como crackear el DES con una maquina especial.

El diseño consistía en un Chip especial que probaba 50 millones de claves DES por segundo hasta que encontraba la correcta, estos chips podían producirse por $10.50 U.S. cada uno, y Wiener había desarrollado una maquina especial que reunía 57000 de estos chips a un costo de un millón de dólares.

La maquina era capaz de crackear cualquier clave DES en menos de siete horas promediando 3.5 horas por clave. Por 10 millones Wiener construía una maquina que tardaba 21 minutos por clave. Y por 100 millones el tiempo se

reducía a dos minutos por clave. Desde ese momento el DES de 56 bits no volvió a ser utilizado con propósitos serios de encriptación de datos.

Un posible sucesor del DES es una versión conocida como Triple-DES que usa dos claves DES para encriptar tres veces, alcanzando un rendimiento equivalente a una única clave de 112 bits, obviamente este nuevo esquema es tres veces mas lento que el DES común.

El algoritmo que sucedió al DES y que es actualmente utilizado por el PGP entre otros es el IDEA (International data encription algorithm).

IDEA usa claves de 128 bits y esta basado en el concepto de "mezclar operaciones de distintos grupos algebraicos". Es mucho mas rápido en sus implementaciones que el DES. Al igual que el DES puede ser usado como cipher-feedback (CFB) o cipher-block-chaining (CBC). EL PGP lo utiliza en modo CFB de 64 bits.

El algoritmo IPES/IDEA fue desarrollado en ETH Zurich por James Massey y Xuejia Lai y publicado por primera vez en 1990. IDEA ha resistido ataques mucho mejor que otros cifradores como FEAL, REDOC-II, LOKI, Snefru y Khafre. Biham y Shamir han sometido al algoritmo IDEA a técnicas de criptoanálisis sin encontrar hasta el momento debilidad alguna en el algoritmo. Grupos de criptoanálisis de varios países se encuentran abocados a atacar el algoritmo para verificar su confiabilidad.

Los principales inconvenientes que presenta DEs son:

- Se considera un secreto nacional de EEUU, por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en software fuera de ese país sin permiso específico del Departamento de Estado.
- La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero

con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se cree que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.

- No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.
- La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente textos elegidos, ya que existe un sistema matemático, llamado Criptoanálisis Diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.

Entre sus ventajas cabe citar:

- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es muy rápido y fácil de implementar.
- Desde su aparición nunca ha sido roto con un sistema práctico.

Ciptosistema Triple DES.

Como hemos visto, el sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (**TDES**), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:

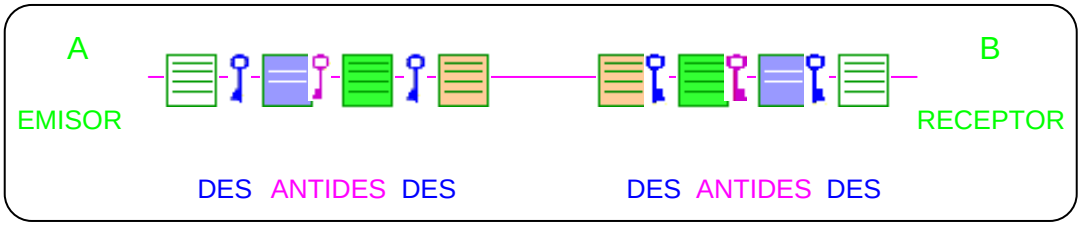


Figura 9: Triple DES

1. Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
2. Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
3. Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

Si la clave de 128 bits está formada por dos claves iguales de 64 bits (C1=C2), entonces el sistema se comporta como un DES simple.

Tras un proceso inicial de búsqueda de compatibilidad con DES, que ha durado 3 años, actualmente TDES usa 3 claves diferentes, lo que hace el sistema mucho más robusto, al conseguirse longitudes de clave de 192 bits (de los cuales son efectivos 168), mientras que el uso de DES simple no está aconsejado.

Sistemas de clave pública.

Los sistemas de encriptación de datos por clave publica han revolucionado el mundo de la criptografía y se han impuesto ampliamente en el mercado de las comunicaciones, la idea aunque sencilla recién surgió en la década del '70, los expertos en criptografía no logran ponerse de acuerdo en cual fue el motivo que demorara tanto el surgimiento de este tipo de sistema de encriptación.

La idea de los sistemas de clave pública es sencilla: cada usuario genera 2 (dos) claves: una publica y una privada, el usuario debe conservar su clave privada a salvo mientras que la clave pública es distribuida en forma masiva.

El juego de claves funciona de la siguiente forma: los mensajes que son encriptados con la clave pública de un usuario solo pueden ser des encriptados con la clave privada del mismo.

El algoritmo de encriptación es publico, de forma tal que cualquiera pueda encriptar un mensaje, el algoritmo de desencriptación debe de forma tal que sin la clave privada sea muy difícil desencriptar el código mientras que con la clave privada esto es una tarea sencilla. Todos los algoritmos de encriptación por clave pública se basan en algún problema en general de tipo matemático de cuyo tiempo de resolución no pueda establecerse una cota inferior.

Knapsacks.

El primer ejemplo sobre el cual presentaremos a los sistemas de clave publica esta basado en un problema de ingenio denominado 'el problema de la mochila'

'El problema de la mochila'.

Se tiene una mochila con capacidad para "K" kilos. Además se cuenta con una lista de "n" objetos cuyos pesos se conocen y son (A1,A2,A3,...,AN). El problema consiste en seleccionar una cierta cantidad de objetos de la lista de forma tal que la mochila quede completamente llena.

Para resolver este problema no se conoce ningún método mejor que el ir probando las distintas combinaciones de objetos y ver si en alguna de ellas la mochila queda completamente llena. Si los pesos de los objetos están en un vector (A1,A2,A3,...,AN) una combinación puede escribirse como un numero binario de N bits en el cual un uno en la posición "i" indica que el elemento "i" debe estar en la mochila, un cero indica lo contrario.

Ej:

A=(3,45,6,7,21,12,9,90)

C1=(00000001)=90

C2=(10101010)=3+6+21+9=39

etc...

De esta forma se puede ver claramente que la cantidad de combinaciones a probar es 2^N siendo N el numero de elementos del vector, a este tipo de vectores lo denominaremos 'Knapsack'. Si N es un numero lo suficientemente grande (por ejemplo 300) la cantidad de combinaciones a probar es tan grande que resultaría imposible probarlas todas antes de que se termine el universo.

Veamos como podemos construir un sistema de clave pública utilizando Knapsacks.

Empecemos por inventar un sistema de clave privada que utilice 'Knapsacks'

Dado un mensaje lo pasamos a binario y tomamos bloques de "N" bits de acuerdo al tamaño del Knapsack, sumamos los elementos del Knapsack que corresponden a los bits en 1 y el número resultante es la codificación del bloque.

Ej: Con bloques de 8 bits y usando el código ASCII si el vector es:

(3, 45, 6, 7, 21, 12, 9,90)

'H' = 01001000 = 45 + 21 = 66

'o' = 01101111 = 45 + 6 + 21 + 12 + 9 + 90 = 183

'l' = 01101100 = 45 + 6 + 21 + 12 = 84

'a' = 01100001 = 45 + 6 + 90 = 141

'Hola' = 66, 183, 84,141

Hasta ahora tenemos un método para encriptar un mensaje, la clave privada por el momento es el Knapsack, sin embargo este sistema tiene un problema: el receptor 'legal' del mensaje pese a poseer el Knapsack aun tiene que resolver el problema de la mochila para poder descifrar el mensaje, esto obviamente dista mucho de ser lo deseado. La solución consiste en simplificar el problema de la mochila utilizando un vector superincrementante (super increasing). Un vector superincrementante es aquel en el cual el elemento Ak es mayor a la sumatoria de todos los elementos con subíndice menor que él.

Ej: (1, 3, 5, 11, 21, 44, 87, 175, 349,701) es superincrementante.

Con un vector super-incrementante resolver el problema de la mochila es fácil, para un cierto numero lo que hay que hacer es tomar el primer elemento del vector menor o igual al numero y poner su bit en 1, luego al número restarle el elemento y con el resultado repetir el procedimiento hasta que el número se hace cero.

Supongamos que tenemos el numero 734.

Para 734: Como 734 > 701 => el bit numero 10 es 1

734-701 = 33

Para 33: 33 > 21 => el bit 5 es 1

33-21 = 12

Para 12 : 12 > 11 => el bit 4 es 1

12-11 = 1

Para 1 : El bit 1 es 1

Luego 734=(1001100001) = 1+11+21+701

El algoritmo de desencriptado, como puede verse, es ahora muy sencillo. El problema es que el sistema sigue siendo de clave privada, conociendo el Knapsack se puede tanto encriptar como desencriptar cualquier mensaje.

Convirtiendo los Knapsacks en un sistema de clave pública.

Lo que debemos lograr es identificar cual va a ser la clave privada y cual va a ser la clave publica, para ello una vez que tenemos un vector superincrementante lo que se hace es elegir dos números t y m forma tal que t y m no tengan factores en común.

Al número t lo denominamos multiplicador.

Al número m lo denominamos modulo.

Además debemos encontrar un número t' que sea el inverso multiplicativo de t usando aritmética módulo m.

Ejemplo: Sea m=1590 Verificar que 1590 y 43 no tienen factores en común

t=43 (43 es primo y 1590 no es divisible por 43)

1590 y 43 son relativamente primos.

Para el inverso de t hacemos 1591/43 = 37 luego t'=37

(37 * 43 = 1591, 1591 mod 1590 = 1)

Ahora lo que hacemos es aplicarle a cada elemento Ai del Knapsack la función

Ai'= Ai*t mod m

(1, 3, 5, 11,21,44,87,175,349,701)=>(43,129,215,473,903,302,561,1165,697,1523)

Al vector que obtenemos una vez aplicada la función lo utilizaremos como clave publica (notar que el vector obtenido no es superincrementante). Es decir que para encriptar un mensaje utilizaremos el método que ya hemos descripto utilizando la clave publica. Si el mensaje cifrado es interceptado el interceptor tiene que resolver el problema de la mochila para poder desencriptar el mensaje, y como sabemos este problema le va a llevar mucho mas que toda su vida.

La clave privada esta formada por t' y m, el receptor legal del mensaje primero convierte todos los números haciendo c*t' mod m y luego convierte el Knapsack de la misma forma, lo único que le resta hacer es resolver el problema de la mochila con un vector superincrementante, lo cual es fácil.

Ej:

Para el Knapsack ejemplo anterior la clave publica es (tomando solo 8 elementos para no hacer tantas cuentas, obviamente cuanto mayor es el vector mas seguro es el sistema)

P = (43, 129, 215, 473, 903, 302, 561,1165)

Supongamos que queremos encriptar 'Hola'

'H' = 01001000 = 129 + 903 = 1032

'o' = 01101111 = 129 + 215 + 903 + 302 + 561 + 1165 = 3275

'l' = 01101100 = 129 + 215 + 903 + 302 = 1549

'a' = 01100001 = 129 + 215 + 1165 = 1509

'Hola' = 1032, 3275, 1549,1509

Si este código es interceptado y sabiendo la clave publica no puede hacerse nada para desencriptar el mensaje pues la clave publica no es superincrementante (aquí reside la gracia del asunto).

La clave privada es t'=37 m=1590

Para desencriptar usamos la clave privada:

1032 * 37 mod 1590 = 24

3275 * 37 mod 1590 = 335

1549 * 37 mod 1590 = 73

1509 * 37 mod 1590 = 183

A continuación se convierte el vector público en un vector superincrementante utilizando la misma transformación.

Luego con los números (24, 335, 73,183) y el vector superincrementante se puede desencriptar fácilmente el mensaje.

El futuro estándar[17].

El NIST de EEUU, en busca de un nuevo sistema de encriptación simétrico que reúna las características funcionales y de seguridad necesarias, decidió convocar en 1977 un concurso a nivel mundial, invitando a los principales desarrolladores de este tipo de sistemas a crear un algoritmo que pueda ser tomado como estándar para los próximos años.

Este nuevo sistema de llamará **AES** (Advanced Encryption Standard), y el algoritmo que utilice se denominará **AEA** (Advanced Encryption Algorithm).

A este concurso se presentaron numerosos autores, y tras un largo proceso de selección el ha seleccionado como futuro estándar el denominado Rijndael, creado por los belgas Vincent Rijmen y Joan Daemen.

---

[17] Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1998.

Rijndael es un cifrador de bloque que opera con bloques y claves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits. El resultado intermedio del cifrado se denomina Estado, que puede representarse como una matriz de bytes de cuatro filas.

A partir de ésta base se realiza una serie de bucles de cifrado, cada uno de ellos consistente en las siguientes operaciones:

1. Sustitución de bytes no lineal, operando independientemente sobre cada uno de los bytes del Estado.
2. Desplazamiento de las filas del Estado cíclicamente con offsets diferentes.
3. Mezcla de columnas, que se realiza multiplicando las columnas del Estado módulo x4+1, consideradas como polinomios en GF(28), por un polinomio fijo c(x).
4. Adición de la clave de vuelta, en la que se aplica al Estado por medio de un simple XOR. La clave de cada vuelta se deriva de la clave de cifrado mediante el esquema de clave.

El esquema de clave consiste en dos operaciones, expansión de clave y selección de clave de vuelta de cifrado, y el proceso de cifrado consta de tres pasos: una adición inicial de la clave de vuelta, n-1 vueltas de cifrado y una vuelta final.

Problemas con las claves[18].

Cualquiera de nosotros sabe por propia experiencia el problema que deriva de tener que administrar y proteger numerosas claves, necesarias para acceder e los diferentes servicios que el trabajo en red nos ofrece.

Una persona cualquiera puede tener asignada una clave para su tarjeta de crédito, otra para su acceso a su estación de trabajo, otra para su acceso al

[18] Ford, James. “Quantum Cryptography Tutorial” Dartmouth College. 1996.

programa de correo, etc., etc. Y tiene que acordarse de todas, y evitar que personas extrañas las conozcan.

Sin duda alguna los sistemas criptográficos nos ayudan sobremanera a la hora de establecer comunicaciones privadas con otra persona, pero acarrean el problema de la administración de claves. Además, usar una misma clave para muchas operaciones es peligroso, ya que conforme pasa el tiempo es cada vez más probable que alguien acceda a la clave, con el consiguiente peligro que esto conlleva.

Tanto es así que, por ejemplo, muchos administradores de una red o sistema obligan a los usuarios de la misma a cambiar obligatoriamente sus claves de acceso, estableciendo unas fechas de caducidad para ellas.

Los sistemas asimétricos no representan ningún problema a la hora de cambiar las claves, ya que la distribución de las claves públicas es abierta, con lo que en seguida podrán acceder a las nuevas claves los usuarios interesados.

Pero en los sistemas simétricos el cambio de la clave origina un trastorno considerable, ya que deberemos distribuir esa nueva clave a todos los usuarios con los que deseemos comunicarnos con seguridad. Y además deberemos hacerlo empleando sistemas de llave pública, como Diffie-Hellman o RSA.

Para solventar estos problemas es cada vez más frecuente el uso de sistemas alternativos, entre los que destaca el conocido como **One Time Password, OTP**, (contraseña de un sólo uso) o de **clave de sesión**. En éste el computador emisor genera una clave aleatoria cada vez que se establece una sesión entre emisor y receptor, que se envía de A a B encriptada con la llave pública de B, para posteriormente efectuar todo el proceso de comunicación cifrada usando esta clave temporal. Si se cae la sesión es necesario reinicializar el proceso, generando una nueva OTP (Obsérvese la figura 10).

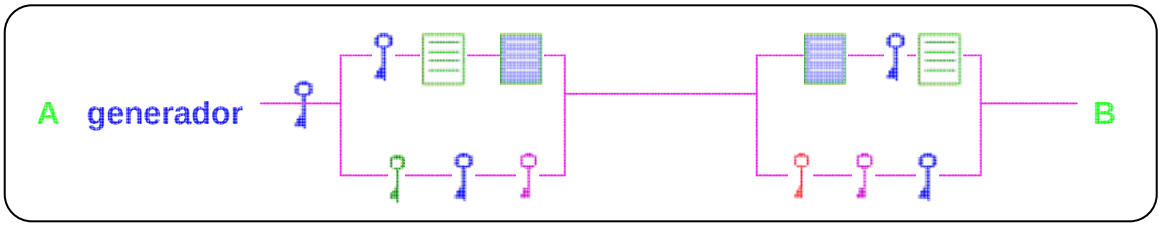


Figura 10: OTP

Este es el sistema que suelen seguir las entidades bancarias y muchas tiendas virtuales, además de ser parte importante de sistemas de comunicación seguros como SSL y SET.

Para poder entender como funcionan estos sistemas de encriptación y cual es su aplicación, en la siguiente tabla mostramos las herramientas de seguridad más utilizadas en los Sistemas de Información actualmente:

HERRAMIENTA	DESCRIPCIÓN
OpenBSD	El sistema operativo preventivamente seguro
TCP Wrappers	Un mecanismo de control de acceso y registro clásico basado en IP
pwdump3	Permite recuperar las hashes de passwords de Windows localmente o a través de la red aunque syskey no esté habilitado
LibNet	Una API (toolkit) de alto nivel permitiendo al programador de aplicaciones construir e inyectar paquetes de red
IpTraf	Software para el monitoreo de redes de IP
Fping	Un programa para el escaneo con ping en paralelo
Bastille	Un script de fortalecimiento de seguridad Para Linux, Max Os X, y HP-UX
Winfingerprint	Un escáner de enumeración de Hosts/Redes para Win32
TCPTraceroute	Una implementación de traceroute que utiliza paquetes de TCP
Shadow Security Scanner	Una herramienta de evaluación de seguridad no-libre
pf	El filtro de paquetes innovador de OpenBSD
LIDS	Un sistema de detección/defensa de intrusiones para el kernel

	Linux
hfnetchk	Herramienta de Microsoft para evaluar el estado de los parches de todas las máquinas con Windows en una red desde una ubicación central
etherape	Un monitor de red gráfico para Unix basado en etherman
dig	Una útil herramienta de consulta de DNS que viene de la mano con Bind
Crack / Cracklib	El clásico cracker de passwords locales de Alec Muffett
cheops / cheops-ng	Nos provee de una interfaz simple a muchas utilidades de red, mapea redes locales o remotas e identifica los sistemas operativos de las máquinas
zone alarm	El firewall personal para Windows. Ofrecen una versión gratuita limitada
Visual Route	Obtiene información de traceroute/whois y la grafica sobre un mapa del mundo
The Coroner's Toolkit (TCT)	Una colección de herramientas orientadas tanto a la recolección como al análisis de información forense en un sistema Unix
tcpreplay	una herramienta para reproducir {replay} archivos guardados con tcpdump o con snoop a velocidades arbitrarias
snoop	Un cantante de rap bastante conocido (Snoop Dogg)! También es un sniffer de redes que viene con Solaris
putty	Un excelente cliente de SSH para Windows
pstools	Un set de herramientas de línea de comandos gratuito para administrar sistemas Windows (procesar listados, ejecución de comandos, etc)
arpwatch	Se mantiene al tanto de las equivalencias entre direcciones ethernet e IP y puede detectar ciertos trabajos sucios

Tabla 9.

2.3.3 SISTEMA DE ENCRIPTACIÓN DE DATOS DE MICROSOFT WINDOWS XP[19].

Este apartado nos muestra detalladamente las funciones de seguridad utilizadas por la compañía Microsoft para su producto Windows XP, objeto de nuestro estudio.

Función:
Sistema encriptador de archivos (EFS) con soporte para multiusuarios.

Descripción:

Encripta cada archivo con una clave generada aleatoriamente. Los procesos de encriptación y desencriptación son transparentes para el usuario. Con Windows XP Professional, EFS ahora soporta la capacidad de que varios usuarios tengan acceso a un documento encriptado.

Beneficio:

El Sistema de archivos encriptados ofrece un alto nivel de protección contra piratas y robo de información.

Función:
Seguridad IP (IPSec).

Descripción:

Ayuda a proteger los datos que se transmiten a través de una red. IPSec es parte importante, debido a que proporcionar seguridad para redes privadas virtuales (VPNs), que permiten a las organizaciones transmitir datos de manera segura por Internet.

[19] http://www.ita.com.ar/winxp/

Beneficio:

Los administradores de informática podrán desarrollar redes privadas virtuales seguras, en forma rápida y fácil.

Función:

Soporte de Kerberos.

Descripción:

Proporciona autenticación de acuerdo con los estándares de la industria y con gran solidez para un registro rápido y único a los recursos corporativos basados en Windows 2000. Kerberos es un estándar de Internet, especialmente efectivo para redes que tienen distintos sistemas operativos, como UNIX.

Beneficio:

Windows XP Professional ofrecerá una firma digital única a los usuarios de recursos y aplicaciones soportadas, que están alojadas tanto en Windows 2000 como en nuestra plataforma de servidor con el nombre código “Whistler”, así como plataformas UNIX soportadas.

Función:

Soporte para tarjetas inteligentes.

Descripción:

Windows XP Professional integra capacidades de tarjetas inteligentes en el sistema operativo, incluyendo soporte para el registro de Tarjetas inteligentes a sesiones de servidores de terminal alojadas en los servidores de terminal basados

en el Servidor “Whistler” (la versión de servidor que da seguimiento a Windows 2000).

Beneficio:

Las tarjetas inteligentes mejoran las soluciones de software, tales como autenticación del cliente, conexión interactiva, firma de código y correo electrónico seguro.

2.4 MEDIOS DE ALMACENAMIENTO MASIVO.

Para los Sistemas de Información uno de los problemas principales es encontrar la infraestructura idónea para el almacenamiento de datos y de información, aquí presentamos los arreglos de discos duros más comunes para el almacenamiento de grandes cantidades de información.

SAN.

Una **red de área de almacenamiento**, en inglés **SAN** (Storage Area Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de respaldo principalmente, está basada en tecnología **fibre channel** y más recientemente en **iSCSI**. Su función es la de conectar de manera rápida, segura y confiable los distintos elementos que la conforman.

Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA, SATA y SCSI. En otros métodos de almacenamiento, (como SMB o NFS), el servidor solicita un determinado fichero, p.ej."/home/usuario/rocks".

En una SAN el servidor solicita "el bloque 6000 del disco 4". La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN,

aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan tradicionalmente en grandes main frames como en IBM, SUN o HP. Aunque recientemente con la incorporación de Microsoft se ha empezado a utilizar en máquinas con sistemas operativos Microsoft.

Antecedentes.

La mayoría de las SAN usan el protocolo SCSI para la comunicación entre los servidores y los dispositivos de almacenamiento, aunque no se haga uso del interfaz físico de bajo nivel. En su lugar se emplea una capa de mapeo, como el estándar FCP.

Sin embargo, la poca flexibilidad que este provee, así como la distancia que puede existir entre los servidores y los dispositivos de almacenamiento, fueron los detonantes para crear un medio de conexión que permitiera compartir los recursos, y a la vez incrementar las distancias y capacidades de los dispositivos de almacenamiento.

Dada la necesidad de compartir recursos, se hizo un primer esfuerzo con los primeros sistemas que compartían el almacenamiento a dos servidores, como el actual HP MSA500G2, pero la corta distancia y la capacidad máxima de 2 servidores, sugirió la necesidad de otra forma de conexión.

Comparativas.

Una SAN se puede considerar una extensión de Direct Attached Storage (DAS). Donde en DAS hay un enlace punto a punto entre el servidor y su almacenamiento, una SAN permite a varios servidores acceder a varios dispositivos de almacenamiento en una red compartida.

Tanto en SAN como en DAS, las aplicaciones y programas de usuarios hacen sus peticiones de datos al sistema de ficheros directamente. La diferencia reside en la manera en la que dicho sistema de ficheros obtiene los datos

requeridos del almacenamiento. En DAS, el almacenamiento es local al sistema de ficheros, mientras que en SAN, el almacenamiento es remoto.

SAN utiliza diferentes protocolos de acceso como Fibre Channel y Gigabit Ethernet. En el lado opuesto se encuentra la tecnología Network-attached storage (NAS), donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos CIFS y Network File System (NFS).

Híbrido SAN-NAS.

Aunque la necesidad de almacenamiento es evidente, no siempre está claro cuál es la solución adecuada en una determinada organización. Elegir la solución correcta puede ser una decisión con notables implicaciones, aunque no hay una respuesta correcta única, es necesario centrarse en las necesidades y objetivos finales específicos de cada usuario u organización.

Por ejemplo, en el caso concreto de las empresas, el tamaño de la compañía es un parámetro a tener en cuenta. Para grandes volúmenes de información, una solución SAN sería más acertada. En cambio, pequeñas compañías utilizan una solución NAS. Sin embargo, ambas tecnologías no son excluyentes y pueden convivir en una misma solución.

Como se muestra en la figura 11, hay una serie de resultados posibles que implican la utilización de tecnologías DAS, NAS y SAN en una misma solución.

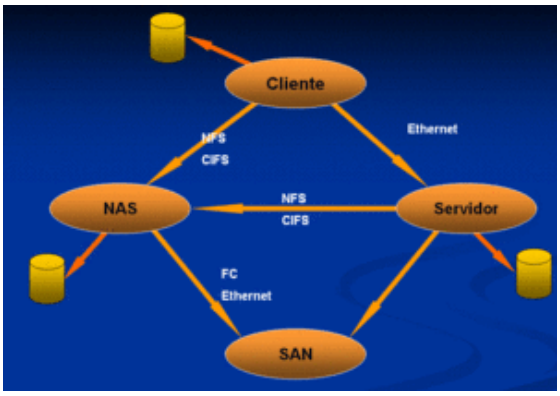


Figura 11: Posibles configuraciones

Características.

Latencia:

Una de las diferencias y principales características de las SAN es que son construidas para minimizar el tiempo de respuesta del medio de transmisión.

Conectividad:

Permite que múltiples servidores sean conectados al mismo grupo de discos o librerías de cintas, permitiendo que la utilización de los sistemas de almacenamiento y los respaldos sean óptimos.

Distancia:

Las SAN al ser construidas con fibra óptica heredan los beneficios de ésta, por ejemplo, las SAN pueden tener dispositivos con una separación de hasta 10 Km sin ruteadores.

Velocidad:

El rendimiento de cualquier sistema de computo dependerá de la velocidad de sus subsistemas, es por ello que las SAN han incrementado su velocidad de transferencia de información, desde 1 Gigabit, hasta actualmente 2 y 4 Gigabits por segundo.

Disponibilidad:

Una de las ventajas de las SAN es que al tener mayor conectividad, permiten que los servidores y dispositivos de almacenamiento se conecten más de una vez a la SAN, de esta forma, se pueden tener *rutas* redundantes que a su vez incrementaran la tolerancia a fallos.

Seguridad:

La seguridad en las SAN ha sido desde el principio un factor fundamental, desde su creación se notó la posibilidad de que un sistema accediera a un dispositivo que no le correspondiera o interfiriera con el flujo de información, es por ello que se ha implementado la tecnología de zonificación, la cual consiste en que un grupo de elementos se aíslen del resto para evitar estos problemas, la zonificación puede llevarse a cabo por hardware, software o ambas, siendo capaz de agrupar por puerto o por WWN (World Wide Name), una técnica adicional se implementa a nivel del dispositivo de almacenamiento que es la Presentación, consiste en hacer que una LUN (Logical Unit Number) sea accesible sólo por una lista predefinida de servidores o nodos (se implementa con los WWN)

Componentes:

Los componentes primarios de una SAN son: switches, directores, HBAs, Servidores, Ruteadores, Gateways, Matrices de discos y Librerías de cintas.

Topología:

Cada topología provee distintas capacidades y beneficios las topologías de SAN son:

Cascada (cascade)

Anillo (ring)

Malla (meshed)

Núcleo/borde (core/edge)

ISL (Inter Switch Link, enlace entre conmutadores):

Actualmente las conexiones entre los switches de SAN se hacen mediante puertos tipo "E" y pueden agruparse para formar una troncal (trunk) que permita mayor flujo de información y tolerancia a fallos.

Arquitectura:

Channel´s actuales funcionan bajo dos arquitecturas básicas, FC-AL (Fibre Channel Arbitrated Loop) y Switched Fabric, ambos esquemas pueden convivir y ampliar las posibilidades de las SAN. La arquitectura FC-AL puede conectar hasta 127 dispositivos, mientras que switched fabric hasta 16 millones teóricamente.

Ventajas:

Compartir el almacenamiento simplifica la administración y añade flexibilidad, puesto que los cables y dispositivos de almacenamiento no necesitan moverse de un servidor a otro. Debemos darnos cuenta de que salvo en el modelo de SAN file system y en los cluster, el almacenamiento SAN tiene una relación de uno a uno con el servidor. Cada dispositivo (o Logical Unit Number *LUN*) de la SAN es "propiedad" de una sola computadora o servidor.

Como ejemplo contrario, NAS permite a varios servidores compartir el mismo conjunto de ficheros en la red. Una SAN tiende a maximizar el aprovechamiento del almacenamiento, puesto que varios servidores pueden utilizar el mismo espacio reservado para crecimiento.

RAID.

En informática, el acrónimo **RAID** (originalmente del inglés ***Redundant Array of Inexpensive Disks***, 'conjunto redundante de discos baratos', en la actualidad también de ***Redundant Array of Independent Disks***, 'conjunto redundante de discos independientes', hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos.

Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor *throughput* (rendimiento) y mayor capacidad.

En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAIDs suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad.

Debido al decremento en el precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipsets de las placas base, los RAIDs se encuentran también como opción en las computadoras personales más avanzadas. Esto es especialmente frecuente en las computadoras dedicadas a tareas intensivas de almacenamiento, como edición de audio y vídeo.

La especificación RAID original sugería cierto número de «niveles RAID» o combinaciones diferentes de discos. Cada una tenía ventajas y desventajas

teóricas. Con el paso de los años, han aparecido diferentes implementaciones del concepto RAID.

La mayoría difiere sustancialmente de los niveles RAID idealizados originales, pero se ha conservado la costumbre de llamarlas con números. Esto puede resultar confuso, dado que una implementación RAID 5, por ejemplo, puede diferir sustancialmente de otra. Los niveles RAID 3 y RAID 4 son confundidos con frecuencia e incluso usados indistintamente.

La misma definición de RAID ha estado en disputa durante años. El uso de término «redundante» hace que muchos objeten sobre que el RAID 0 sea realmente un RAID. De igual forma, el cambio de «barato» a «independiente» confunde a muchos sobre el pretendido propósito del RAID. Incluso hay algunas implementaciones del concepto RAID que usan un solo disco.

Pero en general, diremos que cualquier sistema que emplee los conceptos RAID básicos de combinar espacio físico en disco para los fines de mejorar la fiabilidad, capacidad o rendimiento es un sistema RAID.

Historia.

A Norman Ken Ouchi de IBM le fue concedida en 1978 la Patente USPTO nº 4,092,732, titulada «Sistema para recuperar datos almacenados en una unidad de memoria averiada» (*System for recovering data stored in failed memory unit*), cuyas demandas describen los que más tarde sería denominado escritura totalmente dividida (*full striping*).

Esta patente de 1978 también menciona la copia espejo (*mirroring* o *duplexing*), que más tarde sería denominada RAID 1, y la protección con cálculo de paridad dedicado, que más tarde sería denominada RAID 4, que eran ya arte previo en aquella época.

La tecnología RAID fue definida por primera vez en 1987 por un grupo de informáticos de la Universidad de California, Berkeley. Este grupo estudió la

posibilidad de usar dos o más discos que aparecieran como un único dispositivo para el sistema.

En 1988, los niveles RAID 1 a 5 fueron definidos formalmente por David A. Patterson, Garth A. Gibson y Randy H. Katz en el ensayo «Un Caso para Conjuntos de Discos Redundantes Económicos (RAID)» —*A Case for Redundant Arrays of Inexpensive Disks (RAID)*—, publicado en la Conferencia SIGMOD de 1988 (págs. 109-116). El término «RAID» se usó por vez primera en este ensayo, que dio origen a toda la industria de los conjuntos de discos.

Implementaciones.

La distribución de datos en varios discos puede ser gestionada por hardware dedicado o por software. Además, existen sistemas RAID híbridos basados en software *y* hardware específico.

Con la implementación por software, el sistema operativo gestiona los discos del conjunto a través de una controladora de disco normal (IDE/ATA, Serial ATA, SCSI, SAS o Fibre Channel). Considerada tradicionalmente una solución más lenta, con el rendimiento de las CPUs modernas puede llegar a ser más rápida que algunas implementaciones hardware, a expensas de dejar menos tiempo de proceso al resto de tareas del sistema.

Una implementación de RAID basada en hardware requiere al menos una controladora RAID específica, ya sea como una tarjeta de expansión independiente o integrada en la placa base, que gestione la administración de los discos y efectúe los cálculos de paridad (necesarios para algunos niveles RAID).

Esta opción suele ofrecer un mejor rendimiento y hace que el soporte por parte del sistema operativo sea más sencillo (de hecho, puede ser totalmente transparente para éste). Las implementaciones basadas en hardware suelen soportar sustitución en caliente (*hot swapping*), permitiendo que los discos que fallen puedan reemplazarse sin necesidad de detener el sistema.

En los RAIDs mayores, la controladora y los discos suelen montarse en una caja externa específica, que a su vez se conecta al sistema principal mediante una o varias conexiones SCSI, Fibre Channel o iSCSI. A veces el sistema RAID es totalmente autónomo, conectándose al resto del sistema como un NAS.

Los RAIDs híbridos se han hecho muy populares con la introducción de controladoras RAID hardware baratas. En realidad, el hardware es una controladora de disco normal sin características RAID, pero el sistema incorpora una aplicación de bajo nivel que permite a los usuarios construir RAIDs controlados por la BIOS.

Será necesario usar un controlador de dispositivo específico para que el sistema operativo reconozca la controladora como un único dispositivo RAID. Estos sistemas efectúan en realidad todos los cálculos por software (es decir, los realiza la CPU), con la consiguiente pérdida de rendimiento, y típicamente están restringidos a una única controladora de disco.

Una importante característica de los sistemas RAID por hardware es que pueden incorporar un caché de escritura no volátil (con alimentación de respaldo por batería) que permite aumentar el rendimiento del conjunto de discos sin comprometer la integridad de los datos en caso de fallo del sistema.

Esta característica no está obviamente disponible en los sistemas RAID por software, que suelen presentar por tanto el problema de reconstruir el conjunto de discos cuando el sistema es reiniciado tras un fallo para asegurar la integridad de los datos.

Por el contrario, los sistemas basados en software son mucho más flexibles (permitiendo, por ejemplo, construir RAIDs de particiones en lugar de discos completos y agrupar en un mismo RAID discos conectados en varias controladoras) y los basados en hardware añaden un punto de fallo más al sistema (la controladora RAID).

Todas las implementaciones pueden soportar el uso de uno o más discos de reserva (*hot spare*), unidades preinstaladas que pueden usarse inmediatamente (y casi siempre automáticamente) tras el fallo de un disco del RAID. Esto reduce el tiempo del período de reparación al acortar el tiempo de reconstrucción del RAID.

Se han descrito diversos niveles de arreglos RAID, pero solamente los cinco primeros están realmente operativos. Estos niveles son los siguientes:

- ⇒ RAID 1. Son discos espejo en los cuales se tiene la información duplicada. Tiene los problemas y las ventajas del almacenamiento estable.
- ⇒ RAID 2. Distribuye los datos por los discos, repartiéndolos de acuerdo con una unidad de distribución definida por el sistema o la aplicación. El grupo de discos se usa como un disco lógico, en el que se almacenan bloques lógicos distribuidos según la unidad de reparto.
- ⇒ RAID 3. Reparte los datos a nivel de bit por todos los discos duros. Se puede añadir bits con códigos correctores de error. Este dispositivo exige que las cabezas de todos los discos estén sincronizadas, es decir, que un único disco controlador controle sus movimientos.
- ⇒ RAID 4. Reparto de bloques y cálculo de paridad cada franja de bloques, que se almacena en un disco fijo. En un grupo de cinco discos, por ejemplo, los cuatro primeros serian de datos y el quinto de paridad. Este arreglo tiene el problema de que el disco de paridad se convierte en un cuello de botella y un punto de fallo único.

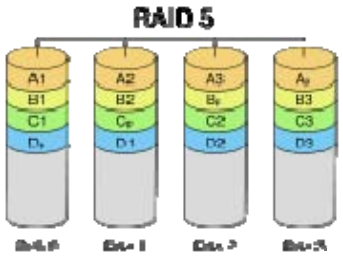


Figura 12: Diagrama de una configuración RAID 5

⇒ RAID 5. Reparto de bloques y paridad por todos los discos de forma cíclica. Tiene la ventaja de la tolerancia a fallos sin los inconvenientes del RAID 4. Actualmente existen múltiples dispositivos comerciales de este estilo y son muy populares en aplicaciones que necesitan fiabilidad (Figura 12).

JBOD (Figura 13).

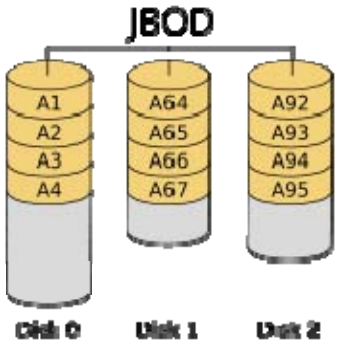


Figura 13: Diagrama de una configuración JBOD

Aunque la **concatenación** de discos (también llamada **JBOD**, de *Just a Bunch Of Drives*, 'Sólo un Montón de Discos') no es uno de los niveles RAID numerados, sí es un método popular de combinar múltiples discos duros físicos en un solo disco virtual. Como su nombre indica, los discos son meramente concatenados entre sí, de forma que se comporten como un único disco.

En este sentido, la concatenación es como el proceso contrario al particionado: mientras éste toma un disco físico y crea dos o más unidades lógicas, JBOD usa dos o más discos físicos para crear una unidad lógica.

Al consistir en un conjunto de discos independientes (sin redundancia), puede ser visto como un primo lejano del RAID 0. JBOD es usado a veces para combinar varias unidades pequeñas (obsoletas) en una unidad mayor con un tamaño útil.

JBOD es parecido al ampliamente usado gestor de volúmenes lógicos LVM y LSM en los sistemas Unix. JBOD es útil para sistemas que no soportan LVM/LSM (como Microsoft Windows, si bien Windows 2003 Server, Windows XP Pro y Windows 2000 soportan JBOD vía software, llamado *spanning* de discos dinámicos). La diferencia entre JBOD y LVM/LSM es que la traducción de la dirección lógica del dispositivo concatenado a la dirección física del disco es realizada por el hardware RAID en el primer caso y por el núcleo en el segundo.

Una ventaja de JBOD sobre RAID 0 es que, en caso de fallo de un disco, en RAID 0 *suele* producirse la pérdida de todos los datos del conjunto, mientras en JBOD sólo se pierden los datos del disco afectado, conservándose los de los restantes discos. Sin embargo, JBOD no supone ninguna mejora de rendimiento.

Network-attached storage.

NAS (del inglés *Network Attached Storage*) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar que un servidor Windows que comparte sus unidades por red es un sistema NAS, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS son basados en ficheros por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en ficheros de pequeño tamaño y gran cantidad. Los protocolos usados son protocolos de compartición de ficheros como NFS, Microsoft Common Internet File System (CIFS).

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Normalmente, estos dispositivos están dispuestos en RAID (*Redundant Arrays of Independent Disks*) o contenedores de almacenamiento redundante.

NAS head.

Un dispositivo hardware simple, llamado «NAS box» o «NAS head», actúa como interfaz entre el NAS y los clientes. Los clientes siempre se conectan al NAS head (más que a los dispositivos individuales de almacenamiento) a través de una conexión Ethernet. NAS aparece en la LAN como un simple nodo que es la dirección IP del dispositivo NAS head.

Estos dispositivos NAS no requieren pantalla, ratón o teclado, sino que poseen interfaz Web.

Comparativas.

El opuesto a NAS es la conexión DAS (Direct Attached Storage) mediante conexiones SCSI o la conexión SAN (Storage Area Network) por fibra óptica, en ambos casos con tarjetas de conexión especificas de conexión al almacenamiento. Estas conexiones directas (DAS) son por lo habitual dedicadas.

En la tecnología NAS, las aplicaciones y programas de usuario hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos CIFS y NFS, y el almacenamiento es local al sistema de ficheros. Sin embargo, DAS y SAN realizan las peticiones de datos directamente al sistema de ficheros.

Las ventajas del NAS sobre la conexión directa (DAS) son la capacidad de compartir las unidades, un menor coste, la utilización de la misma infraestructura de red y una gestión más sencilla. Por el contrario, NAS tiene un menor rendimiento y fiabilidad por el uso compartido de las comunicaciones.

A pesar de las diferencias, NAS y SAN no son excluyentes y pueden combinarse en una misma solución: Híbrido SAN-NAS.

Usos de NAS.

NAS es muy útil para proporcionar de almacenamiento centralizado a computadoras clientes en entornos con grandes cantidades de datos. NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento. El crecimiento del mercado potencial para NAS es el mercado de consumo donde existen grandes cantidades de datos multimedia.

El precio de las aplicaciones NAS ha bajado en los últimos años, ofreciendo redes de almacenamiento flexibles para el consumidor doméstico con costos menores de lo normal, con discos externos USB o FireWire algunas de estas soluciones para el mercado doméstico son desarrolladas para procesadores ARM, PowerPC o MIPS corriendo sistemas operativos Linux empotrado. Ejemplos de estos son Buffalo's TeraStation y Linksys NSLU2.

Sistemas Operativos NAS para usuarios de PC.

Están disponibles distribuciones Software Libre orientadas a servicios NAS, Linux y FreeBSD, incluyendo FreeNAS, NASLite y Openfiler. Son configurables mediante interfaz web y pueden ejecutarse en computadoras con recursos limitados.

Existen distribuciones en LiveCD, en memorias USB o desde una de los discos duros montados en el sistema. Ejecutan Samba (programa), el dominio

Network File System y dominios de FTP que están disponibles para dichos sistemas operativos.

Ata over ethernet.

ATA over Ethernet (**AoE**) es un protocolo de red desarrollado por la compañía Brantley Coile y diseñado para acceder a dispositivos de almacenamiento ATA mediante redes Ethernet. Proporciona la posibilidad de construir redes de almacenamiento (SAN) de bajo costo con tecnologías estándar.

AoE no depende de las capas superiores de Ethernet, tales como IP, UDP, TCP, etc. Esto significa que AoE no es ruteable en LANs y está diseñado únicamente para SAN. Como alternativa a iSCSI, la especificación AoE mide solamente ocho páginas comparado con las 257 páginas de iSCSI.

2.4.1 EL DISCO DURO.

Un disco duro (Figura 14) es un dispositivo que permite el almacenamiento y recuperación de grandes cantidades de información. Los discos duros forman el principal elemento de la memoria secundaria de una computadora, llamada así en oposición a la memoria principal o memoria RAM (Random Access Memory, memoria de acceso aleatorio).

Figura 14

Tanto los discos duros como la memoria principal son memorias de trabajo (varían su contenido en una sesión con la computadora). Sin embargo, presentan importantes diferencias: la memoria principal es volátil (su contenido se borra al

apagar la computadora), muy rápida (ya que se trata de componentes electrónicos) pero de capacidad reducida.

La memoria secundaria, en cambio, es no volátil, menos rápida (componentes mecánicos) y de gran capacidad. La memoria principal contiene los datos utilizados en cada momento por la computadora pero debe recurrir a la memoria secundaria cuando necesite recuperar nuevos datos o almacenar de forma permanente los que hayan variado.

2.4.2 GENERALIDADES SOBRE EL DISCO DURO.

Estructura física de un disco duro.

Elementos de un disco duro.

Un disco duro forma una caja herméticamente cerrada que contiene dos elementos no intercambiables: la unidad de lectura y escritura y el disco como tal. La unidad de lectura y escritura es un conjunto de componentes electrónicos y mecánicos que hacen posible el almacenamiento y recuperación de los datos en el disco.

El disco es, en realidad, una pila de discos, llamados platos, que almacenan información magnéticamente. Cada uno de los platos tiene dos superficies magnéticas: la superior y la inferior. Estas superficies magnéticas están formadas por millones de pequeños elementos capaces de ser magnetizados positiva o negativamente. De esta manera, se representan los dos posibles valores que forman un bit de información (un cero o un uno). Ocho bits contiguos constituyen un byte (un carácter).

Funcionamiento de una unidad de disco duro.

Veamos cuáles son los mecanismos que permiten a la unidad acceder a la totalidad de los datos almacenados en los platos.

En primer lugar, cada superficie magnética tiene asignado uno de los cabezales de lectura/escritura de la unidad. Por tanto, habrá tantos cabezales como caras tenga el disco duro y, como cada plato tiene dos caras, este número equivale al doble de platos de la pila. El conjunto de cabezales se puede desplazar linealmente desde el exterior hasta el interior de la pila de platos mediante un brazo mecánico que los transporta.

Por último, para que los cabezales tengan acceso a la totalidad de los datos, es necesario que la pila de discos gire. Este giro se realiza a velocidad constante y no cesa mientras esté encendida la computadora. En cambio, en los discos flexibles sólo se produce el giro mientras se está efectuando alguna operación de lectura o escritura.

El resto del tiempo, la disquetera permanece en reposo. Con las unidades de CD-ROM ocurre algo similar, sin embargo en este caso la velocidad de giro no es constante y depende de la distancia al centro del dato que se esté leyendo (Figura 15).

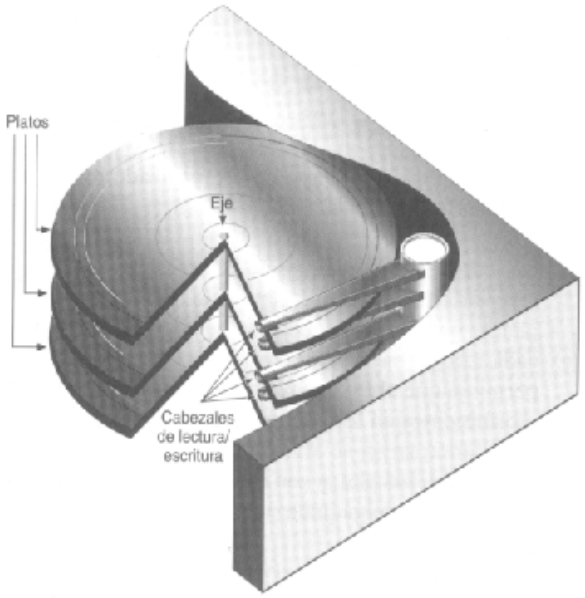


Figura 15

Cada vez que se realiza una operación de lectura en el disco duro, éste tiene que realizar las siguientes tareas: desplazar los cabezales de lectura/escritura hasta el lugar donde empiezan los datos; esperar a que el primer dato, que gira con los platos, llegue al lugar donde están los cabezales; y, finalmente, leer el dato con el cabezal correspondiente. La operación de escritura es similar a la anterior.

Estructura física: cabezas, cilindros y sectores.

Ya hemos visto que cada una de las dos superficies magnéticas de cada plato se denomina cara. El número total de caras de un disco duro coincide con su número de cabezas. Cada una de estas caras se divide en anillos concéntricos llamados pistas. En los discos duros se suele utilizar el término cilindro para referirse a la misma pista de todos los discos de la pila. Finalmente, cada pista se divide en sectores (Figura 16).

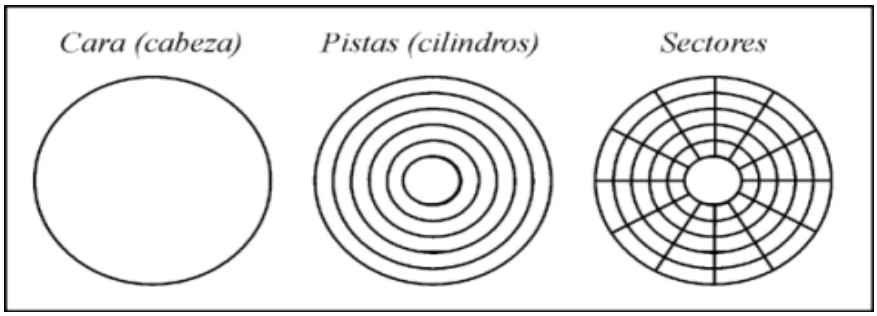


Figura 16

Los sectores son las unidades mínimas de información que puede leer o escribir un disco duro. Generalmente, cada sector almacena 512 bytes de información.

El número total de sectores de un disco duro se puede calcular: nº sectores = nº caras * nº pistas/cara * nº sectores/pista. Por tanto, cada sector queda unívocamente determinado si conocemos los siguientes valores: cabeza, cilindro y sector. Por ejemplo, el disco duro ST33221A de Seagate tiene las siguientes especificaciones: cilindros = 6.253, cabezas = 16 y sectores = 63.

El número total de sectores direccionables es, por tanto, 6.253*16*63 = 6.303.024 sectores. Si cada sector almacena 512 bytes de información, la capacidad máxima de este disco duro será de 6.303.024 sectores * 512 bytes/sector = 3.227.148.228 bytes ~ 3 GB.

Las cabezas y cilindros (Figura 17) comienzan a numerarse desde el cero y los sectores desde el uno. En consecuencia, el primer sector de un disco duro será el correspondiente a la cabeza 0, cilindro 0 y sector 1.

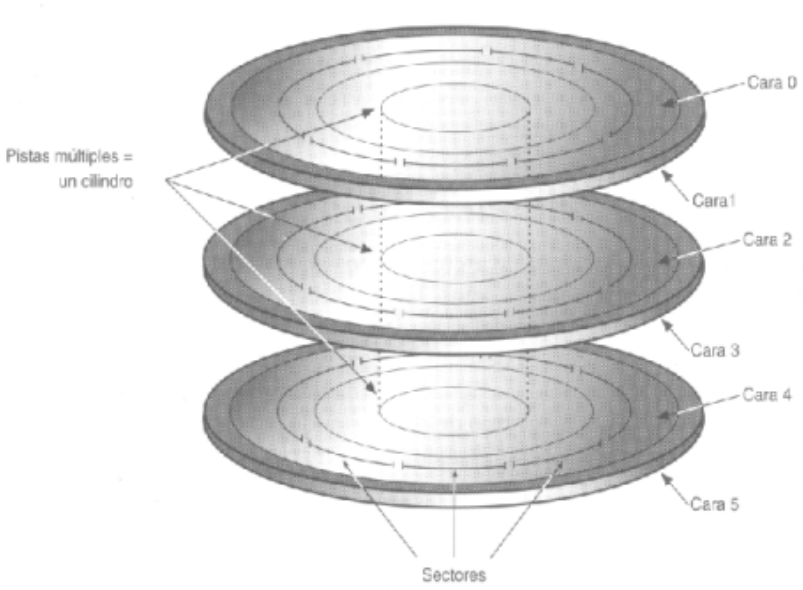


Figura 17

Estructura lógica de un disco duro.

La estructura lógica de un disco duro está formada por:

- ✓ El sector de arranque (Master Boot Record).
- ✓ Espacio particionado.
- ✓ Espacio sin particionar.

El sector de arranque es el primer sector de todo disco duro (cabeza 0, cilindro 0, sector 1). En él se almacena la tabla de particiones y un pequeño programa master de inicialización, llamado también Master Boot. Este programa es el encargado de leer la tabla de particiones y ceder el control al sector de arranque de la partición activa. Si no existiese partición activa, mostraría un mensaje de error.

El espacio particionado, es el espacio del disco que ha sido asignado a alguna partición. El espacio no particionado, es espacio no accesible del disco ya que todavía no ha sido asignado a ninguna partición. A continuación se muestran

ejemplos de la estructura del sistema de archivos para las particiones de un disco duro en diferentes sistemas operativos.

MS-DOS

Boot	Dos copias de la FAT	Directorio raíz	Datos y directorios

UNIX

Boot	Superbloque	Mapa de bits	Nodos-i	Datos y directorios

WINDOWS NT

Boot	Superbloque	Mapa de bits	Descriptores de archivos	Datos y directorios

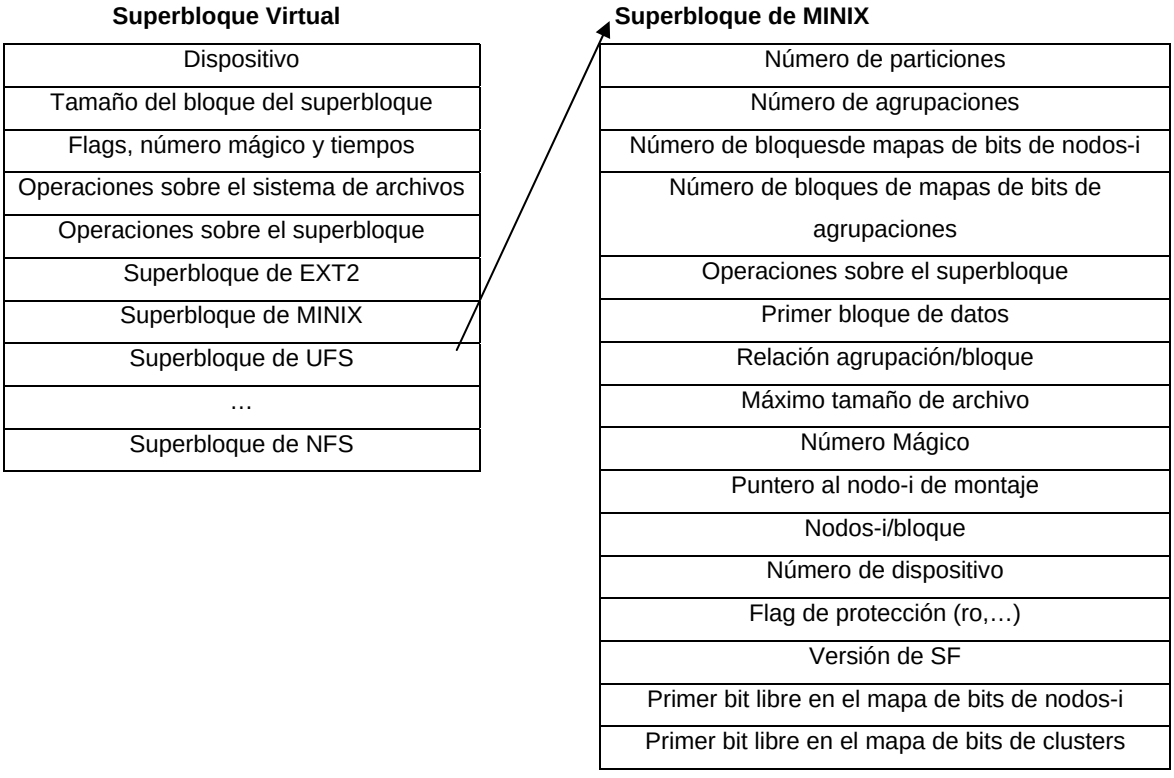


Figura 19

Las particiones.

Cada disco duro constituye una unidad física distinta. Sin embargo, los sistemas operativos no trabajan con unidades físicas directamente sino con unidades lógicas. Dentro de una misma unidad física de disco duro puede haber varias unidades lógicas. Cada una de estas unidades lógicas constituye una partición del disco duro.

Esto quiere decir que podemos dividir un disco duro en, por ejemplo, dos particiones (dos unidades lógicas dentro de una misma unidad física) y trabajar de la misma manera que si tuviésemos dos discos duros (una unidad lógica para cada unidad física).

Particiones y directorios.

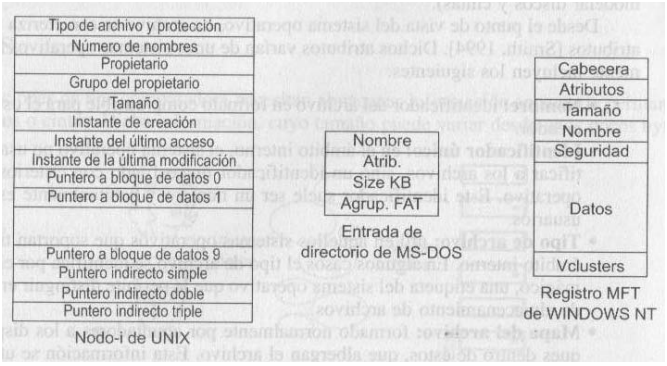
Ambas estructuras permiten organizar datos dentro de un disco duro. Sin embargo, presentan importantes diferencias:

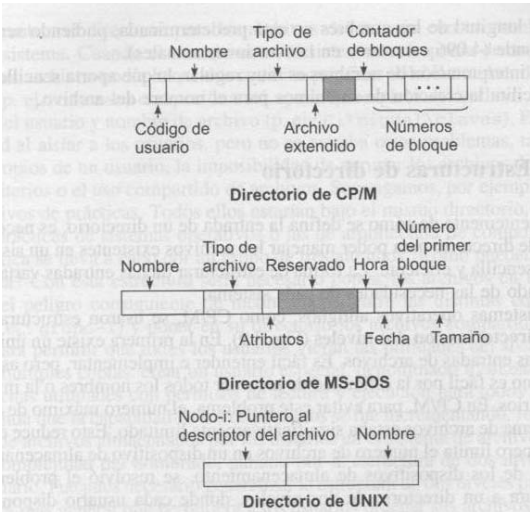
1ª). Las particiones son divisiones de tamaño fijo del disco duro; los directorios son divisiones de tamaño variable de la partición;

2ª). Las particiones ocupan un grupo de cilindros contiguos del disco duro (mayor seguridad); los directorios suelen tener su información desperdigada por toda la partición;

3ª). Cada partición del disco duro puede tener un sistema de archivos (sistema operativo) distinto; todos los directorios de la partición tienen el sistema de archivos de la partición.

Las siguientes imágenes muestran las diferentes formas de representar y almacenar un archivo para que este pueda se manipulado por el sistema operativo y su sistema de archivos correspondiente.





Como mínimo, es necesario crear una partición para cada disco duro. Esta partición puede contener la totalidad del espacio del disco duro o sólo una parte. Las razones que nos pueden llevar a crear más de una partición por disco se suelen reducir a tres.

Razones organizativas.

Considérese el caso de la computadora que es compartido por dos usuarios y, con objeto de lograr una mejor organización y seguridad de sus datos deciden utilizar particiones separadas.

Instalación de más de un sistema operativo. Debido a que cada sistema operativo requiere (como norma general) una partición propia para trabajar, si queremos instalar dos sistemas operativos a la vez en el mismo disco duro (por ejemplo, Windows 98 y Linux), será necesario particionar el disco.

Razones de eficiencia.

Por ejemplo, suele ser preferible tener varias particiones FAT pequeñas antes que una gran partición FAT. Esto es debido a que cuanto mayor es el tamaño de una partición, mayor es el tamaño del grupo (cluster) y, por consiguiente, se desaprovecha más espacio de la partición. Más adelante, explicaremos esto con mayor detalle.

Las particiones pueden ser de dos tipos: primarias o lógicas. Las particiones lógicas se definen dentro de una partición primaria especial denominada partición extendida.

En un disco duro sólo pueden existir 4 particiones primarias (incluida la partición extendida, si existe). Las particiones existentes deben inscribirse en una tabla de particiones de 4 entradas situada en el primer sector de todo disco duro. De estas 4 entradas de la tabla puede que no esté utilizada ninguna (disco duro sin particionar, tal y como viene de fábrica) o que estén utilizadas una, dos, tres o las cuatro entradas.

En cualquiera de estos últimos casos (incluso cuando sólo hay una partición), es necesario que en la tabla de particiones figure una de ellas como partición activa. La partición activa es aquella a la que el programa de inicialización (Master Boot) cede el control al arrancar. El sistema operativo de la partición activa será el que se cargue al arrancar desde el disco duro.

De todo lo anterior se pueden deducir varias conclusiones

Para que un disco duro sea utilizable debe tener al menos una partición primaria. Además para que un disco duro sea arrancable debe tener activada una de las particiones y un sistema operativo instalado en ella. Esto quiere decir que el proceso de instalación de un sistema operativo en la computadora consta de la

creación de su partición correspondiente, instalación del sistema operativo (formateo de la partición y copia de archivos) y activación de la misma.

De todas maneras, es usual que este proceso esté guiado por la propia instalación. Un disco duro no arrancará si no se ha definido una partición activa o si, habiéndose definido, la partición no es arrancable (no contiene un sistema operativo).

Hemos visto antes que no es posible crear más de cuatro particiones primarias. Este límite, ciertamente pequeño, se logra subsanar mediante la creación de una partición extendida (como máximo una). Esta partición se ocupa, al igual que el resto de las particiones primarias, una de las cuatro entradas posibles de la tabla de particiones.

Dentro de una partición extendida se pueden definir particiones lógicas sin límite. El espacio de la partición extendida puede estar ocupado en su totalidad por particiones lógicas o bien, tener espacio libre sin particionar.

Veamos el mecanismo que se utiliza para crear la lista de particiones lógicas. En la tabla de particiones del Master Boot Record debe existir una entrada con una partición extendida (la cual no tiene sentido activar). Esta entrada apunta a una nueva tabla de particiones similar a la ya estudiada, de la que sólo se utilizan sus dos primeras entradas.

La primera entrada corresponde a la primera partición lógica; la segunda, apuntará a una nueva tabla de particiones. Esta nueva tabla contendrá en su primera entrada la segunda partición lógica y en su segunda, una nueva referencia a otra tabla. De esta manera, se va creando una cadena de tablas de particiones hasta llegar a la última, identificada por tener su segunda entrada en blanco.

Particiones primarias y particiones lógicas.

Ambos tipos de particiones generan las correspondientes unidades lógicas de la computadora. Sin embargo, hay una diferencia importante: sólo las particiones primarias se pueden activar. Además, algunos sistemas operativos no pueden acceder a particiones primarias distintas a la suya.

Lo anterior nos da una idea de qué tipo de partición utilizar para cada necesidad. Los sistemas operativos deben instalarse en particiones primarias, ya que de otra manera no podrían arrancar. El resto de particiones que no contengan un sistema operativo, es más conveniente crearlas como particiones lógicas.

Por dos razones: primera, no se malgastan entradas de la tabla de particiones del disco duro y, segunda, se evitan problemas para acceder a estos datos desde los sistemas operativos instalados. Las particiones lógicas son los lugares ideales para contener las unidades que deben ser visibles desde todos los sistemas operativos.

Algunos sistemas operativos presumen de poder ser instalados en particiones lógicas (Windows NT), sin embargo, esto no es del todo cierto: necesitan instalar un pequeño programa en una partición primaria que sea capaz de cederles el control.

Estructura lógica de las particiones.

Un aspecto fundamental en el manejo de datos e información es la forma en que se almacenan en los discos duros, la estructura lógica de cada una de las particiones dependiendo del sistema operativo y la función que este desempeñe, tendrá establecidos sus parámetros de funcionamiento señalados por la empresa que los creó.

Dependiendo del sistema de archivos utilizado en cada partición, su estructura lógica será distinta. En los casos de MS-DOS y Windows 95, está formada por sector de arranque, FAT, copia de la FAT, directorio raíz y área de datos.

De todas formas, el sector de arranque es un elemento común a todos los tipos de particiones (Figura 20).

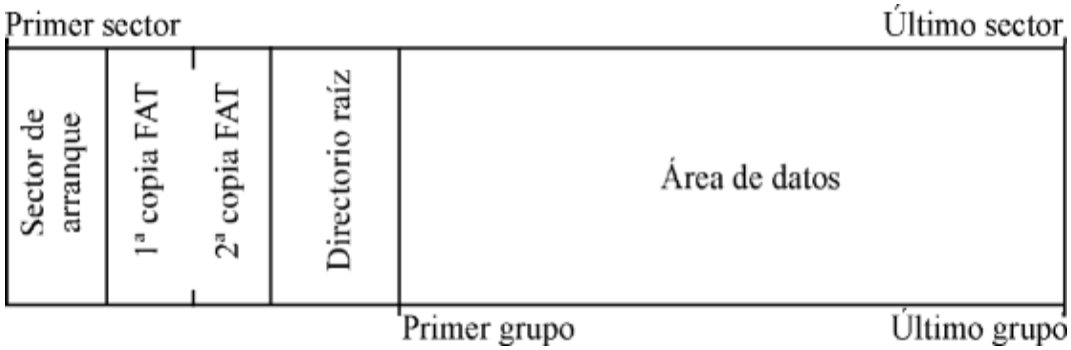


Figura 20

Todas las particiones tienen un sector de arranque (el primero de la partición) con información relativa a la partición. Si la partición tiene instalado un sistema operativo, este sector se encargará de arrancarlo.

Si no hubiese ningún sistema operativo (como es el caso de una partición para datos) y se intentara arrancar, mostraría un mensaje de error.

CAPÍTULO 3

MANUAL DE PROCEDIMIENTOS, TÉCNICAS Y MÉTODOS ESPECIALIZADOS BASADO EN LA NORMA ISO/IEC 27001:2005.

INTRODUCCIÓN

Hasta el momento se ha demostrado el valor que representan los sistemas de información para la vida cotidiana del ser humano, tanto así; como los datos contenidos en ellos, en este capítulo presentamos un manual con el cual podremos mantener seguros los datos que recopilamos en los medios de almacenamiento masivo.

Cable establecer que la mayoría de sistemas operativos cuentan con herramientas y utilerías para administrar, distribuir y proteger los datos que son grabados en los Discos Duros, y en un caso remoto de pérdida de información existen dos formas de recuperarla, que son:

1. Con software dedicado a la recuperación de datos en Discos Duros formateados

2. En laboratorios especializados en recuperar la información grabada en un Disco Duro con “daño físico”.

En lo siguiente se explicará detalladamente los métodos y técnicas más utilizadas para este fin.

3.1 MÉTODOS Y TÉCNICAS PARA EL MANEJO DE LA INFORMACIÓN DE FORMA SEGURA EN EL SISTEMA OPERATIVO WINDOWS XP.

Cuando uno trabaja con computadoras es susceptible a cometer errores por no conocer el correcto manejo de estos equipos, así mismo por fallas que están fuera de nuestro control, para tal efecto se recomiendan los siguientes métodos y técnicas para poder trabajar con sistemas informáticos para no ser víctimas de estos errores y por ende sufrir perdidas de información importante en su momento.

Caso 1.

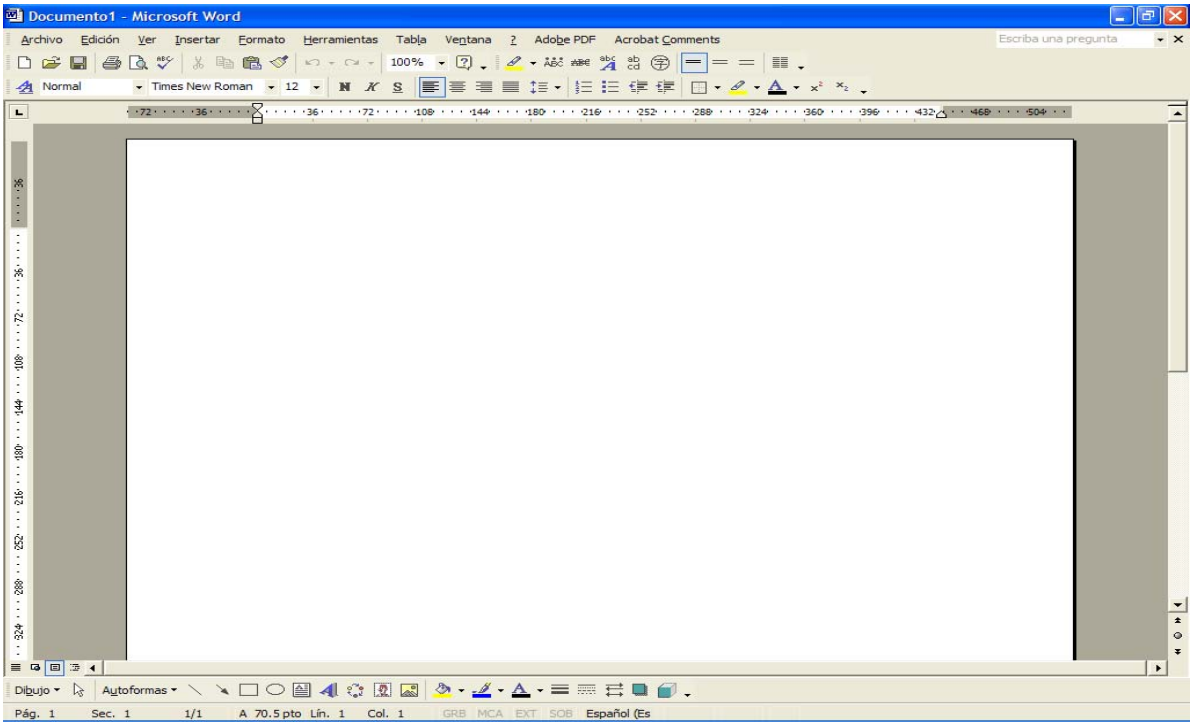
Uso de paquetería comercial: Microsoft Office XP (2003).

La empresa Microsoft System´s, así como tantas otras han tenido a bien facilitar la vida de las personas con la creación de distintos productos computacionales y así lograr incorporarnos al avance tecnológico que día a día se vive en todo el mundo. Dado que el Sistema Operativo más comercial y utilizado es Microsoft Windows (en cualquiera de sus versiones) basaremos nuestro estudio en este Sistema Operativo y en sus utilerías para lograr el resguardo de la información al momento de trabajar con estas.

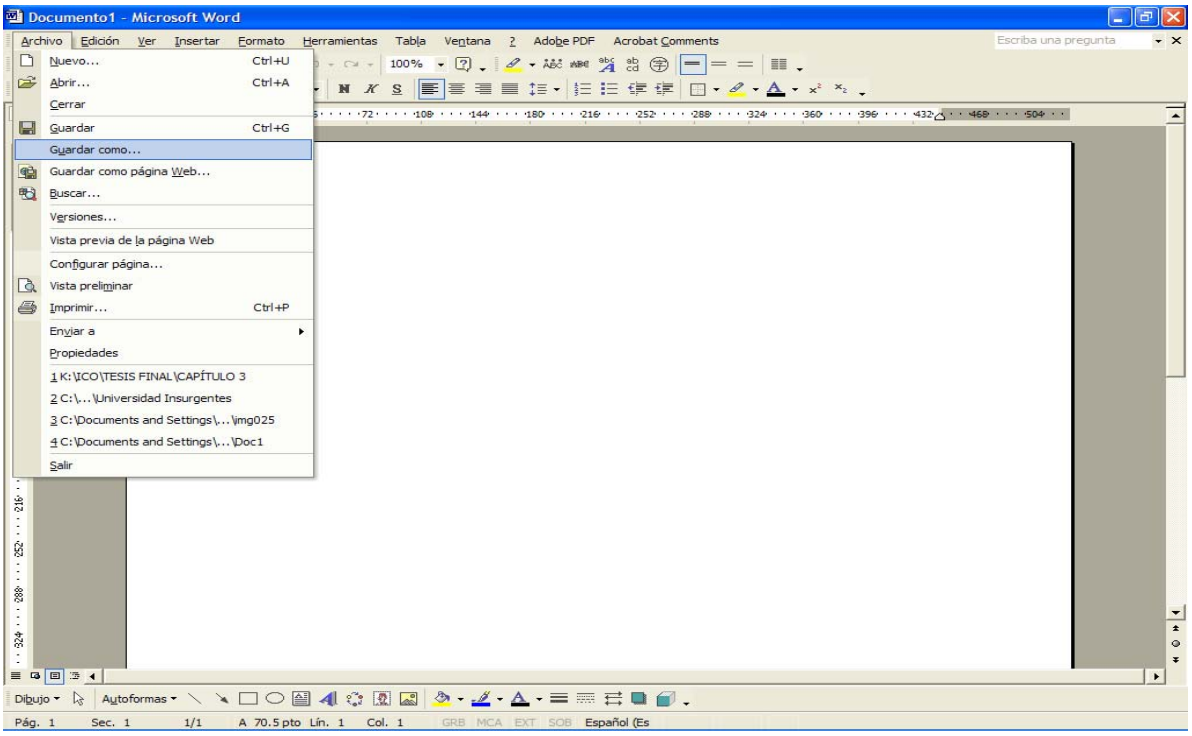
En lo siguiente se describirá por medio de imágenes la manera correcta y segura de trabajar con las utilerías del paquete producido y distribuido por Microsoft System´s denominado Microsoft Office versión XP (2003). Cabe aclarar que se ejemplificará únicamente con la utilería “Microsoft Office Word” ya que para todas las demás contenidas en este paquete se tienen los mismos aspectos de seguridad.

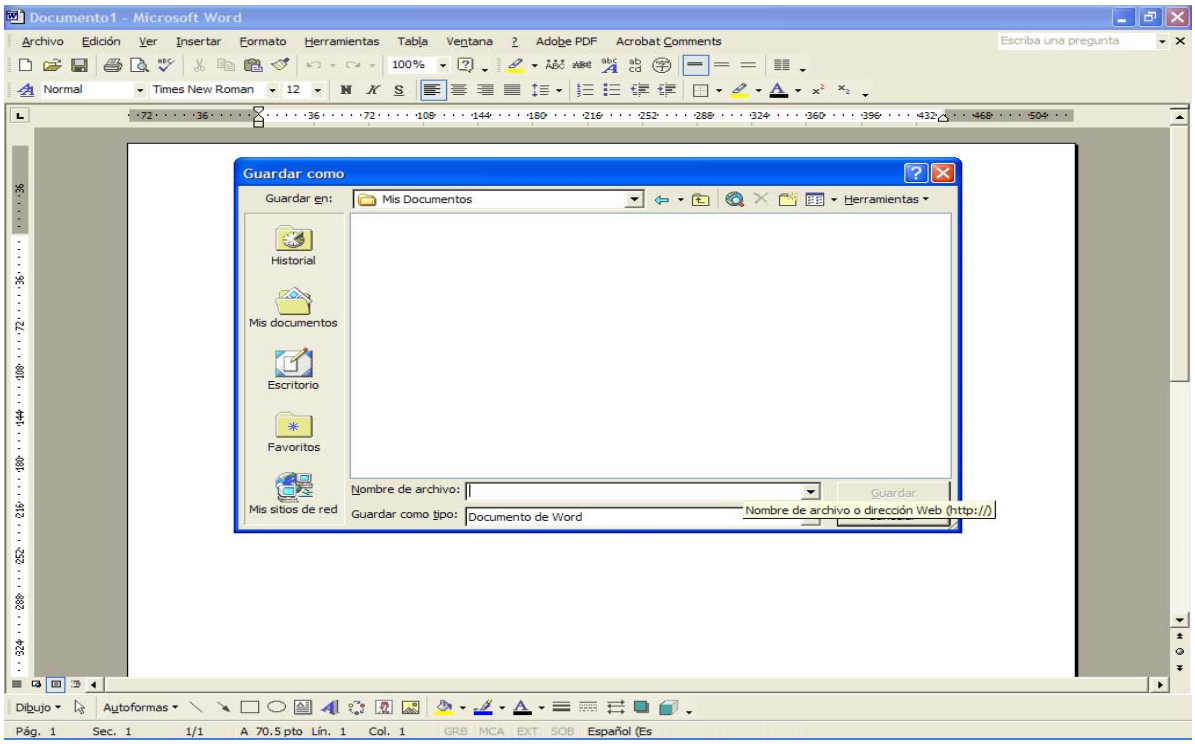
Pantalla principal Microsoft Office Word.

Una vez ya en sesión y realizado el documento procederemos a presentar la manera en la cual debemos guardar los cambios que realicemos para evitar pérdidas de información y poder así obtener los mejores resultados al trabajar con Microsoft Office.

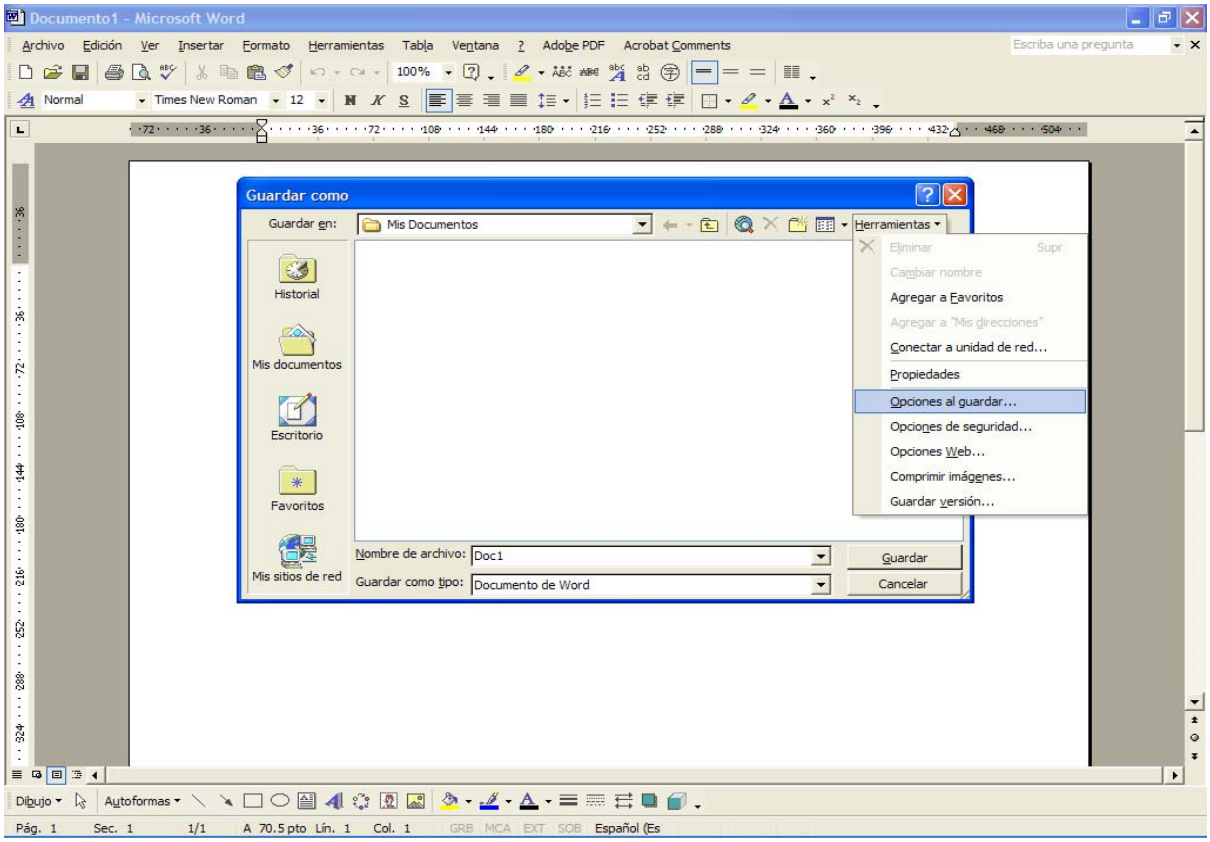


Las siguientes imágenes nos muestran la forma en como debemos guardar un documento nuevo (esto aplica para cualquiera de las utilerías de Microsoft Office), así como los cuadros de dialogo apropiados.


Documento1 - Microsoft Word
Archivo Edición Ver Insertar Formato Herramientas Tabla Ventana ? Adobe PDF Acrobat Comments
Escriba una pregunta
Nuevo... Ctrl+U
Abrir... Ctrl+A
Cerrar
Guardar Ctrl+G
Guardar como...
Guardar como página Web...
Buscar...
Versiones...
Vista previa de la página Web
Configurar página...
Vista preliminar
Imprimir... Ctrl+P
Enviar a
Propiedades
1 K:\ICO\TESIS FINAL\CAPÍTULO 3
2 C:\...\Universidad Insurgentes
3 C:\Documents and Settings\...\img025
4 C:\Documents and Settings\...\Doc1
Salir
Dibujo Autoformas
Pág. 1 Sec. 1 1/1 A 70.5 pto Lín. 1 Col. 1 GRB MCA EXT SOB Español (Es


Documento1 - Microsoft Word
Archivo Edición Ver Insertar Formato Herramientas Tabla Ventana ? Adobe PDF Acrobat Comments
Escriba una pregunta
Normal Times New Roman 12
Guardar como
Guardar en: Mis Documentos
Herramientas
Historial
Mis documentos
Escritorio
Favoritos
Mis sitios de red
Nombre de archivo:
Guardar como tipo: Documento de Word
Guardar
Nombre de archivo o dirección Web (http://)
Dibujo Autoformas
Pág. 1 Sec. 1 1/1 A 70.5 pto Lín. 1 Col. 1 GRB MCA EXT SOB Español (Es

La siguiente imagen nos presenta un submenú poco conocido, pero muy funcional, veamos ¿por qué?



La ventana emergente de este submenú nos presenta la siguiente serie de opciones para guardar un documento de forma personalizada y segura:

- Crear siempre una copia de seguridad:

Nos crea una copia temporal en el Disco Duro en la siguiente dirección: C:\WINDOWS\Temp, con la finalidad de que en un determinado caso fallara el sistema podamos recuperar la información guardada hasta el último instante de la falla.

- Permitir guardar rápidamente.

Indica al sistema que guarde todos los cambios rápidamente y salga del programa.

- Permitir guardar en segundo plano.

Esta función guarda los cambios al documento sin preguntar mientras estamos trabajando con el documento o cualquier otro programa.

- Incrustar fuentes TrueType.

Incrusta cualquier fuente (**TrueType** es un formato estándar de fuentes tipográficas escalables desarrollado inicialmente por Apple Computer a fines de la década de los ochenta para competir comercialmente con el formato "Tipo 1" de Adobe, el cual estaba basado en el lenguaje de descripción de página conocido como PostScript. Una de las principales fortalezas de TrueType era que ofrecía a los diseñadores de fuentes un mayor grado de control (mediante "hints") sobre la forma en que los caracteres se desplegaban en pantalla o en impresos a tamaños menores, con lo cual se lograba una mejor legibilidad).

- Preguntar por las propiedades del documento.

Permite asignarle las siguientes propiedades al documento:

- ✓ Tipo de Archivo.
- ✓ Se abre con:
- ✓ Ubicación.
- ✓ Creado.
- ✓ Modificado.
- ✓ Último Acceso.
- ✓ Atributos:
    - Sólo lectura.
    - Oculto.
    - Archivo.

- Preguntar si se guarda la plantilla Normal.

Cuando inicia cualquier utilería de Microsoft Office, éste carga automáticamente las plantillas y los complementos que se encuentran en las

carpetas Inicio, al activar esta función no será necesario guardar los cambios realizados a las plantillas cargadas por defecto por el programa.

- Guardar datos sólo para formularios.

Esta opción almacena los datos cargados para poder trabajar con formularios (Formulario: documento que contiene espacios en blanco de relleno o campos de formulario, en los que se escribe información) donde por ejemplo se cree un formulario de inscripción en pantalla con listas desplegables en las que los usuarios pueden seleccionar los elementos.

- Incrustar datos lingüísticos.

La característica Incrustar datos lingüísticos determina si se almacena información de corrección de reconocimiento de escritura en el documento cuando es guardado en las versiones 97 a 2003 para dar formato a estas mismas.

- Crear una copia local de los archivos guardados en la red o en las unidades extraíbles.

Para los equipos de cómputo que trabajan en red o que solo son de uso momentáneo (y en su caso aquellos que cuenten con software que no guarda ni permite ningún cambio en la configuración preestablecida) se recomienda esta opción para salvaguardar toda la información con la que estemos trabajando.

- Guardar información de auto recuperación cada: minutos.

Permite tener una copia del archivo (archivo temporal con todos los cambios realizados), después de un determinado tiempo, para evitar pérdida de información.

- Incrustar etiquetas inteligentes.

Cuando esta activada esta opción se genera un reconocimiento de datos en el programa y se marcan los datos con un indicador de etiqueta inteligente con los cuales se podrán ingresar datos de manera eficaz y segura. Cualquiera de los siguientes tipos de información son reconocidos como etiquetas inteligentes:

→ Nombre de personas.
→ Fechas.
→ Horas.
→ Direcciones.
→ Lugares.
→ Números de teléfono.
→ Destinatarios recientes de correo electrónico de Outlook.
→ Símbolos de tableros de cotizaciones.

- Guardar etiquetas inteligentes como propiedades XML en páginas Web

Al crear páginas Web se puede recurrir a las etiquetas inteligentes para facilitar el trabajo y modificación de estas.

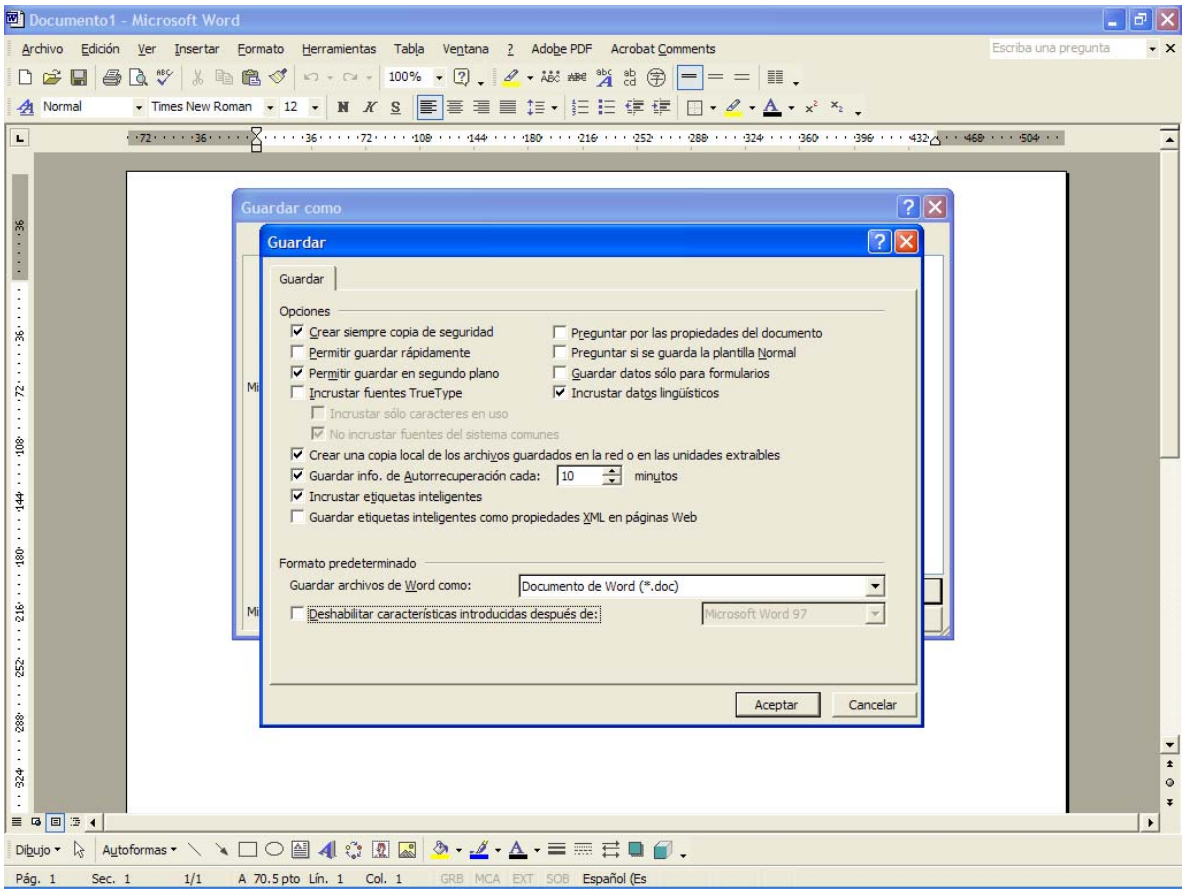
- Formato predeterminado:

- Guardar archivos de Word como:

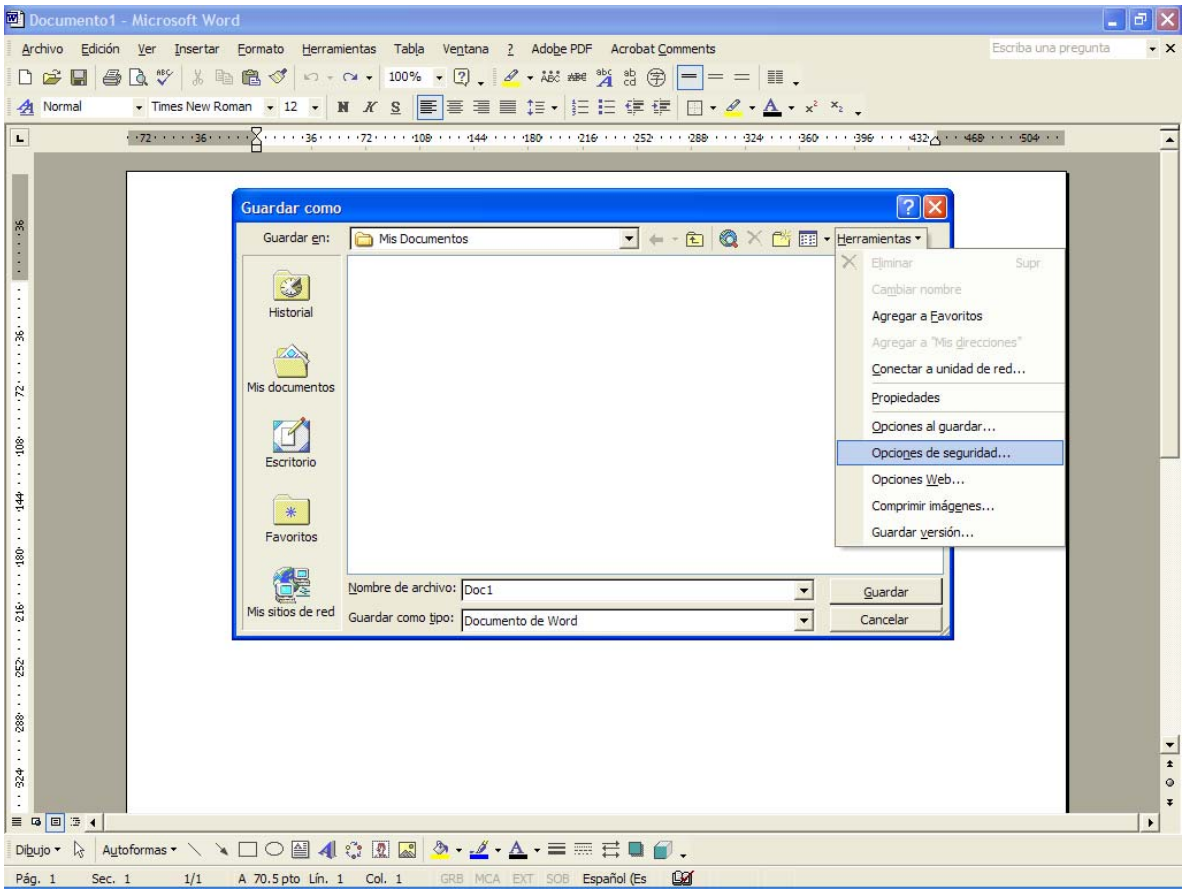
Permite guardar los archivos creados con esta o cualquier otra utilería, para programas compatibles si es que se deseara trabajar con ellos en cualquier otro equipo de cómputo que no contase con esta utilería de Microsoft Office.

- Deshabilitar características introducidas después de:

Deshabilita características de los documentos solo para las versiones indicadas, haciendo que el archivo quede inutilizable para versiones anteriores.



Una vez conocidas las ventajas que Microsoft Office nos ofrece en opciones de guardado podemos analizar las opciones de seguridad con las que cuenta. En la presente imagen se muestra como podemos acceder a estas propiedades.



Ya situados en este submenú (Ver siguiente imagen) nos encontramos las siguientes funciones referentes a la seguridad de los documentos establecida por los usuarios:

- Opciones de cifrado de archivo para este documento:

Contraseña de apertura:

- Opciones de uso compartido de archivo para este documento:

Contraseña de escritura.

Recomendado sólo lectura.

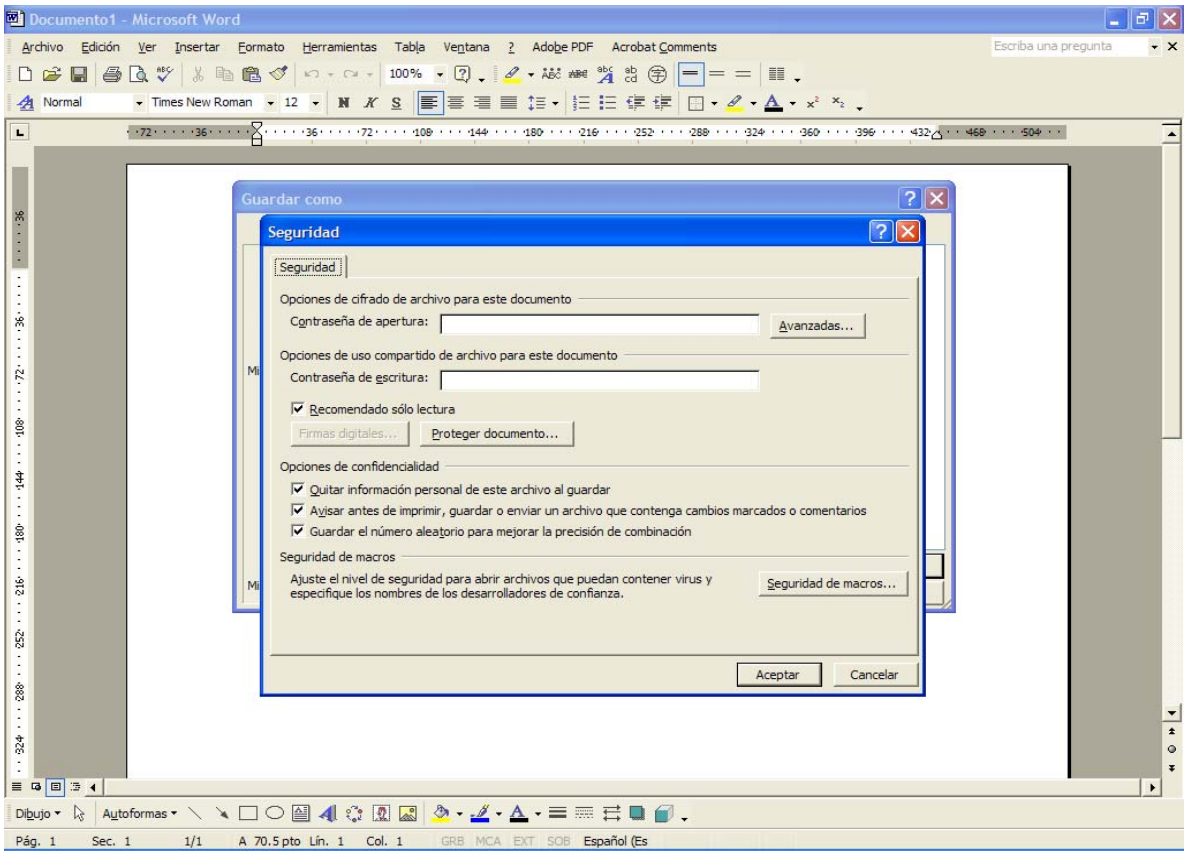
- Opciones de confidencialidad:

Quitar información personal de este archivo al guardar.

Avisar antes de imprimir, guardar o enviar un archivo que contenga cambios marcados o comentarios.

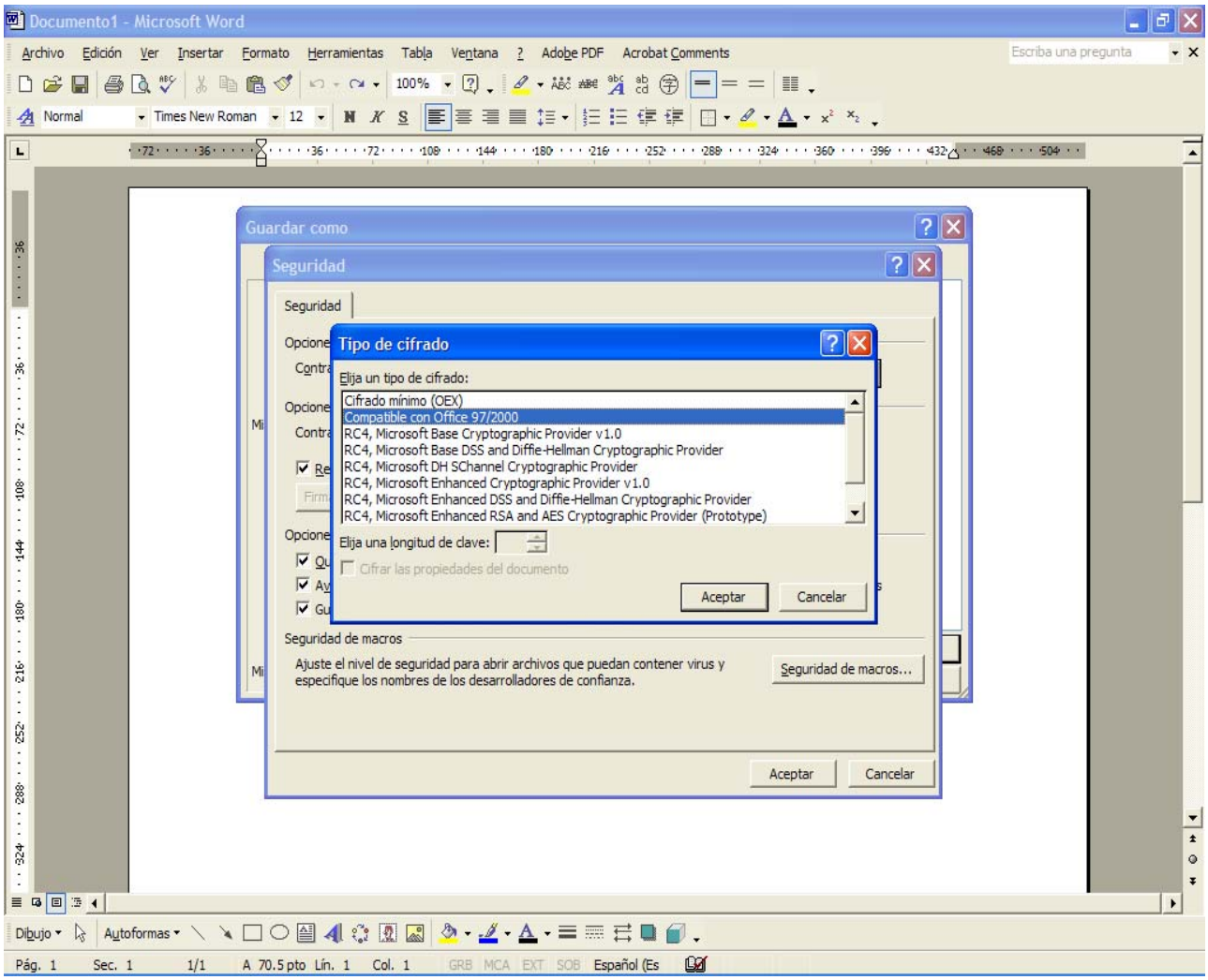
Guardar el número aleatorio para mejorar la precisión de combinación.

- Seguridad de macros.

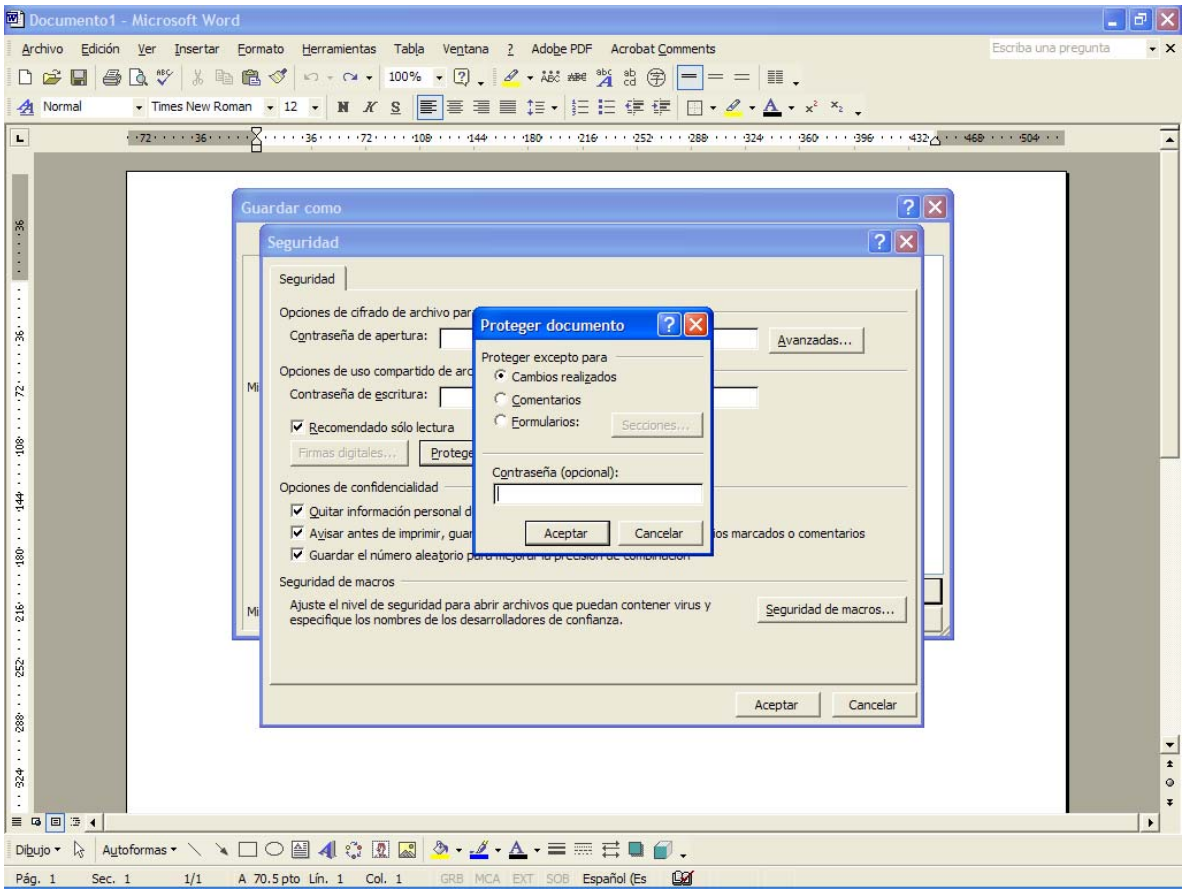


Dentro de las opciones de cifrado de archivo para este documento en la contraseña de apertura tenemos en las opciones avanzadas el tipo de cifrado con el que cuenta Microsoft Office y del cual podemos hacer uso, estos son los siguientes:

- Cifrado Mínimo (OEX)
- Compatible con Office 97/200
- RC4, Microsoft Base Cryptographic Provider v 1.0
- RC4, Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
- RC4, Microsoft DH SChannel Cryptographic Provider
- RC4, Microsoft Enhanced Cryptographic Provider v 1.0
- RC4, Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
- RC4, Microsoft Enhanced RSA and AES Cryptographic (Prototype)
- RC4, Microsoft RSA Channel Cryptographic Provider
- RC4, Microsoft Strong Cryptographic Provider



Una opción más de seguridad proporcionada por Microsoft Office en sus utilerías es la protección de los documentos para que sólo sean para lectura excepto determinadas partes del documento como se muestra en la figura.



Caso 2.

Transferencia de archivos (File Transfer).

El término “File transfer” se refiere a la transferencia de un archivo de un DTE: Data Terminal Equipment (Equipos de Terminal de Datos) a otro. A veces se utiliza la comunicación punto-a-punto (point-to-point communication) que es una conexión que no se interrumpe entre dos equipos de cómputo. Cualquier archivo existe en un sistema de archivos (file system) que es el sistema responsable de la organización y acceso a los archivos guardados en un medio externo, normalmente un Disco Duro. Existen una serie de operaciones que son comunes a los sistemas de archivos:

1. Discos

Medios magnéticos o electrónicos que pueden guardar información. Esta información guardada en un disco es dividida en grupos de bytes llamados

sectores (sectors), que son organizados en anillos en el disco. Un anillo es llamado un track. La información en un disco es leída y escrita por un cabezal de lectura-escritura (read-write head), que se mueve de track a track según el disco rota.

2. Archivos (files)

Consisten de una serie de bytes agrupados en estructuras llamadas record y guardados en uno o más bloques en un disco. El sistema de archivos mantiene un directorio que contiene los nombres de los archivos en el disco. Los atributos asociados a cada archivo son guardados en el disco también.

3. Acceso a archivos (file access)

Como mínimo, las operaciones del sistema de archivos incluyen:

a. Creación del archivo

Antes de que algún archivo sea escrito en disco, éste contiene un directorio vacío y una lista de bloques disponibles. Cuando un archivo se va a crear, el sistema de archivo añade el nombre del nuevo archivo en el directorio, al igual que cualquier otro atributo necesario. Una vez el archivo es creado, se puede escribir en él.

b. Abrir el archivo

Un archivo que existe (uno que tiene nombre en el directorio) es accesado por una aplicación que requiere que se abra, usualmente para leer o escribir en él. Muchos sistemas de archivos verifican los atributos del archivo antes de abrirlo.

c. Cerrar el archivo

Cuando una aplicación ha terminado de acceder un archivo, el sistema de archivos espera que la aplicación lo cierre, para que así el archivo esté disponible para otra aplicación.

d. Leer el archivo

Los archivos son abiertos para lectura para permitir que el proceso accese la información en ellos. El acceso puede ser, por ejemplo, secuencial: se accesa el

próximo record disponible para ser procesado o directo: se puede accesar cualquier record en el archivo.

e. Escribir el archivo

Un archivo también se puede abrir para escribir en él, permitiendo que se actualice la información existente o se añada nueva información.

Protocolos para transferir archivos.

Son las reglas que describen los pasos requeridos para que ocurra la transferencia de archivos. El programa para transferir archivos y el programa de comunicaciones operan por separado, ofreciendo como beneficio:

Portabilidad.

Como el protocolo de transferencia de archivos no hace referencia al protocolo de comunicación, cambiar el último un es transparente para el otro.

Prueba y Verificación.

El número de lugares en donde un error debe ser buscado es reducido grandemente si cada parte del sistema es probado independientemente.

El protocolo de transferencia de archivos describe tres operaciones básicas:

1. Identificación del archivo

El archivo existente debe ser abierto para lectura en un DTE y el nuevo archivo debe ser creado en el otro DTE. En ambos casos, el nombre del archivo y posiblemente su localización se debe especificar en ambos DTEs.

2. Transferencia de records

Una vez el archivo ha sido abierto para su lectura en un DTE (el “source”) y creado para escritura en el otro DTE (el “destination”), su contenido debe ser transferido.

Si el programa de comunicación opera más lento que el de transferencia, se pueden perder algunos datos. Para eso se usa el “handshake” entre el programa

de comunicación y el de transferencia: el programa de transferencia provee otro mensaje solo cuando el programa de comunicaciones lo permite.

Muchos protocolos de transferencia tienen “acknowledgment” a ambos lados de la comunicación, lo que significa que pueden existir dos grupos de “acknowledgment”: el del programa de comunicación y el del programa de transferencia.

No se debe asumir que un mensaje que se recibió correctamente está escrito en el archivo. Es posible que esto no suceda, por ejemplo, si el disco tiene error no podrá escribir el mensaje recibido.

3. Indicador de fin de archivo (end-of-file)

Al transferir el contenido de un archivo, también se envía un indicador de fin de archivo. Por lo general este indicador no se escribe en el archivo, solo es una señal para el programa de transferencia para que cierre el archivo.

3.2 SOFTWARE DEDICADO A LA RECUPERACIÓN DE DATOS EN DISCOS DUROS FORMATEADOS.

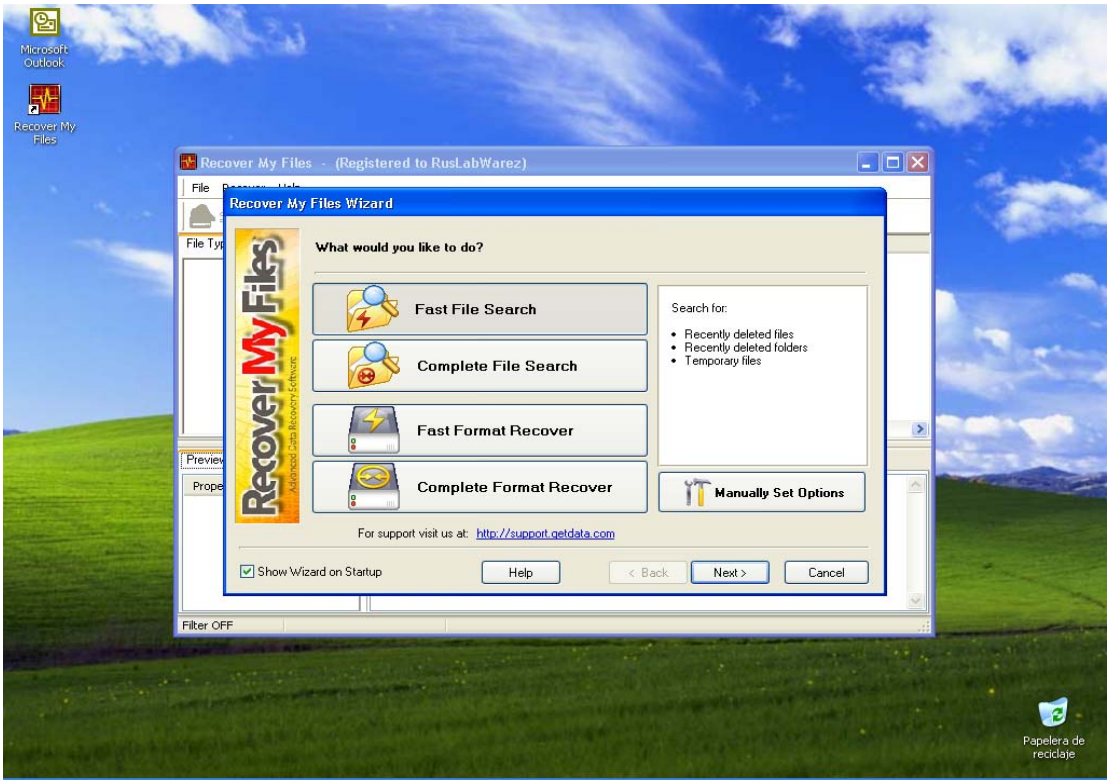
Hasta el momento hemos visto los diferentes métodos y técnicas para mantener segura nuestra información, en este tema mostraremos una técnica especializada para recuperar información de Discos Duros en los cuales se borraron archivos importantes o en un caso extremo que este haya sido formateado.

Cabe aclarar que se eligió este programa ya que cumple con distintos criterios de búsqueda y recuperación de información, pero existen varios más con el mismo fin y diferentes funciones.

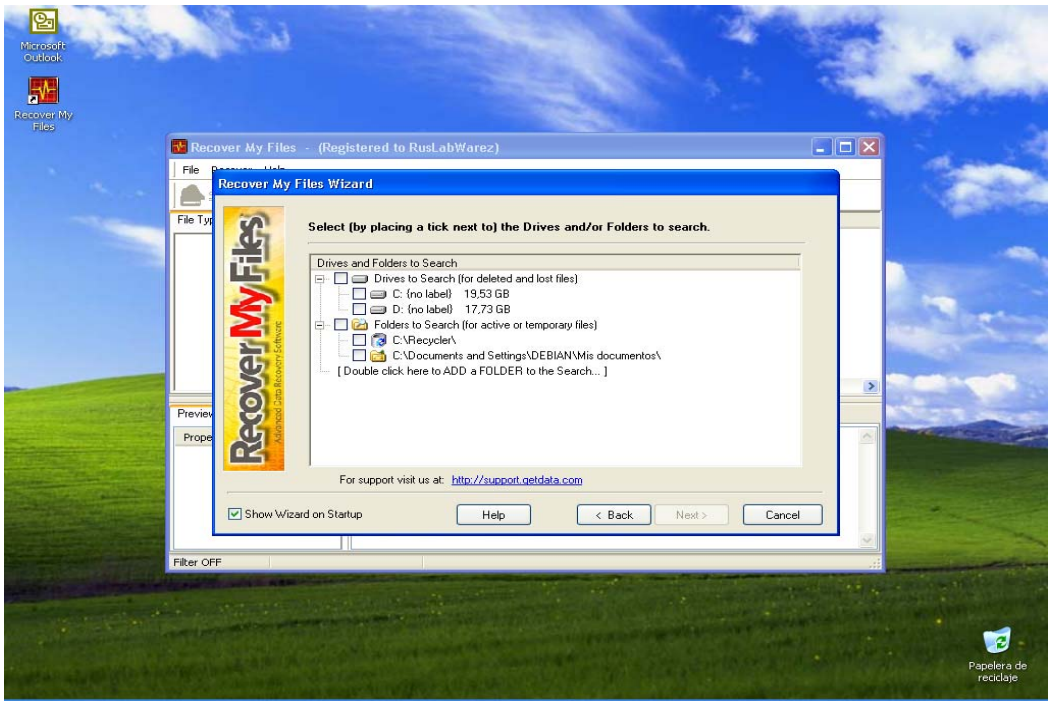
Pantalla principal de Recover My Files de RusLabWarez.

Para explicar el funcionamiento de este programa lo haremos ejemplificando con la búsqueda de archivos rápida, cada imagen muestra el proceso que debemos seguir para poder encontrar y recuperar los archivos que deseamos.

En la pantalla principal seleccionaremos el tipo de búsqueda (que en este caso es búsqueda de archivos rápida) según sean las necesidades de recuperación de archivos.

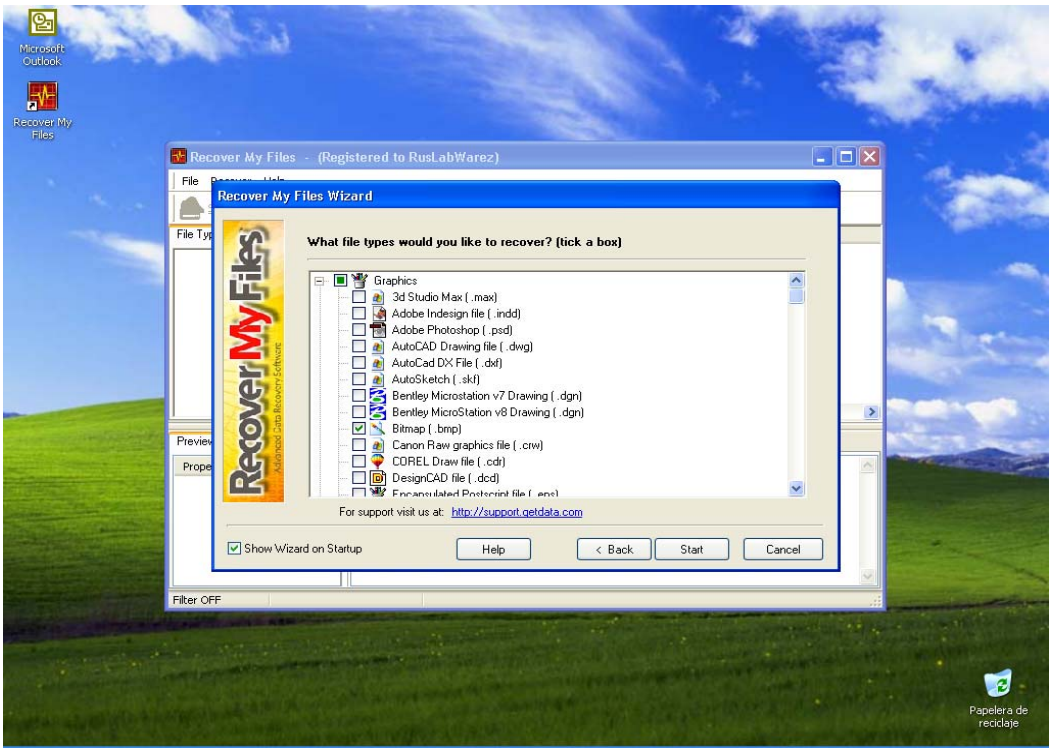


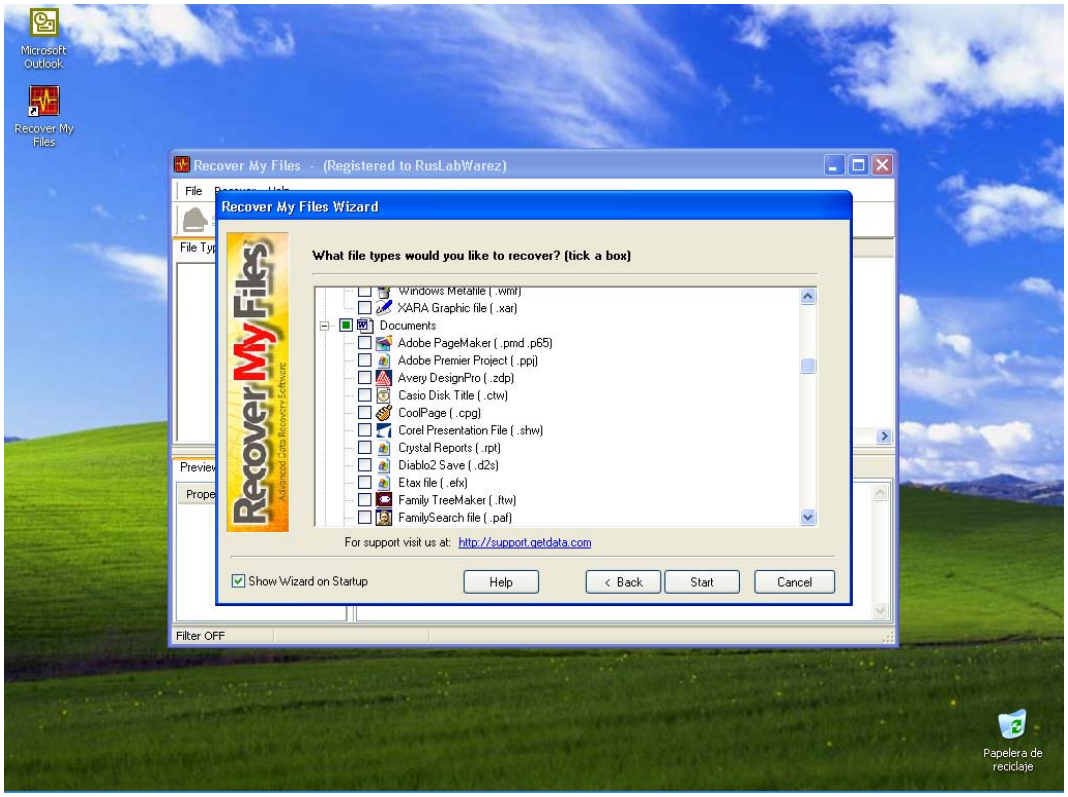
Una vez seleccionada la función nos encontramos con una nueva ventana que nos pide seleccionar (poniendo una señal al lado de) las unidades y/o folders de búsqueda, aquí podemos personalizar la búsqueda de lo que “perdimos”, observe la imagen.

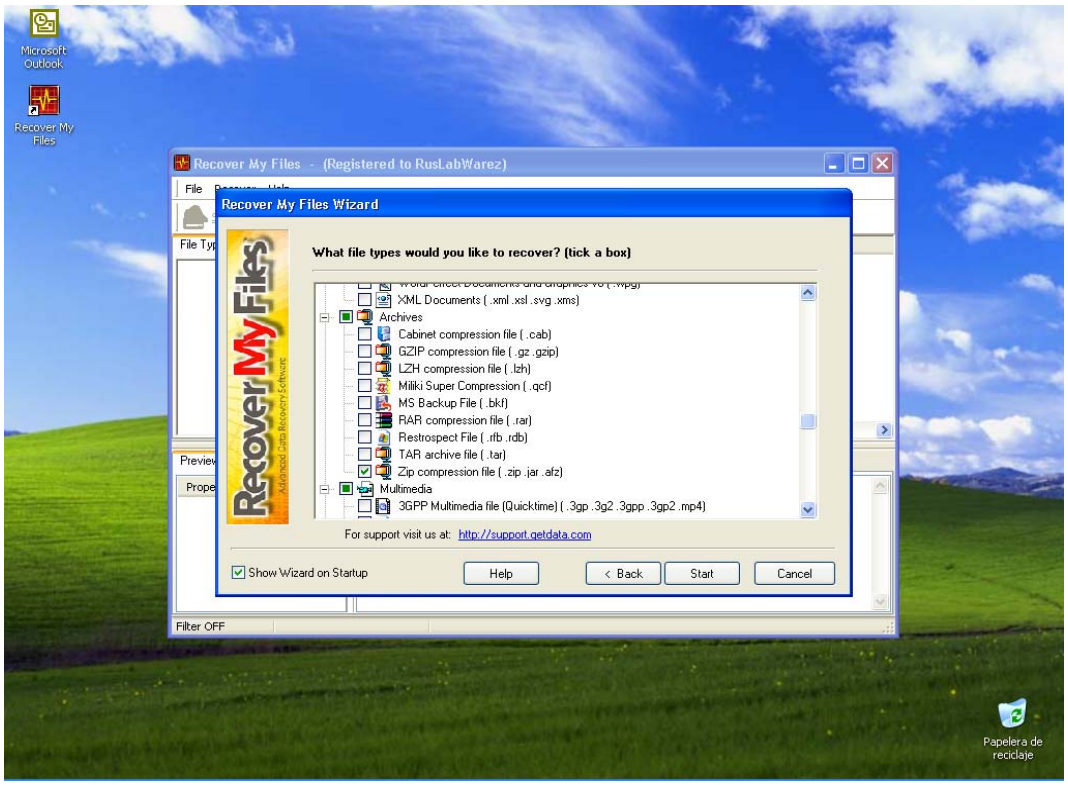


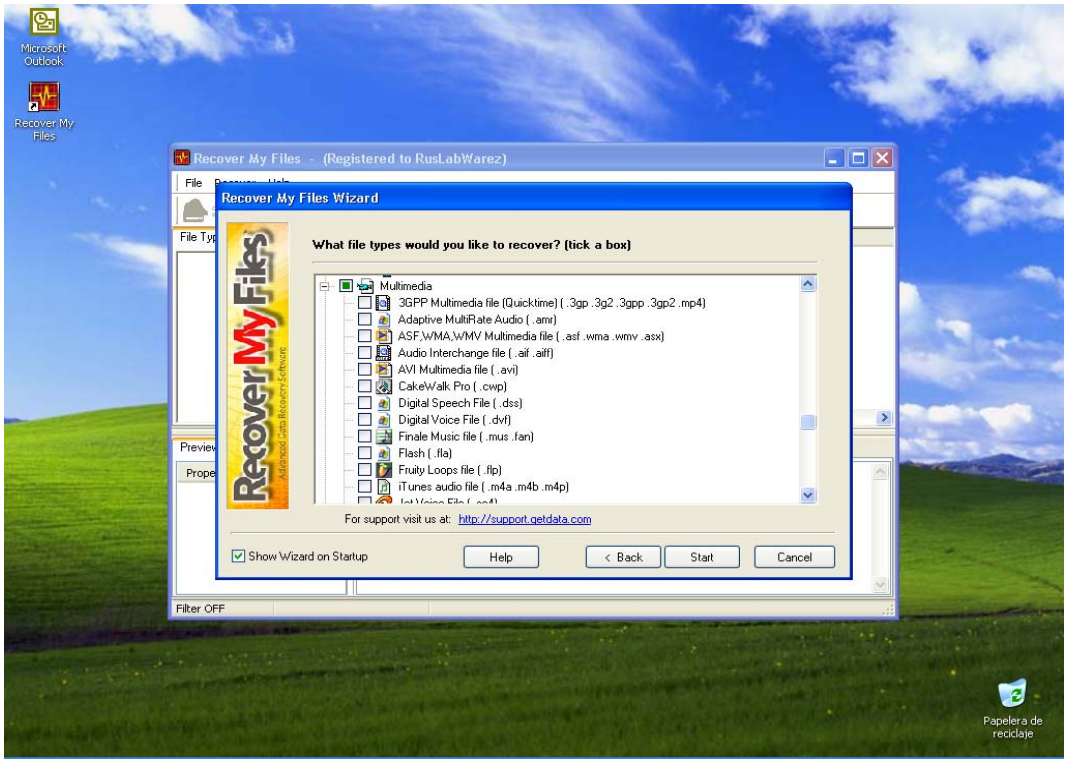
La anterior opción es por si no sabemos con exactitud el archivo que necesitamos recuperar, pero si se sabe con exactitud el tipo de archivo que buscamos lo podemos especificar en la siguiente ventana emergente que nos muestra el programa, nótese que este programa abarca la mayoría de programas con los que pudiéramos realizar un documento, archivo o proyecto.

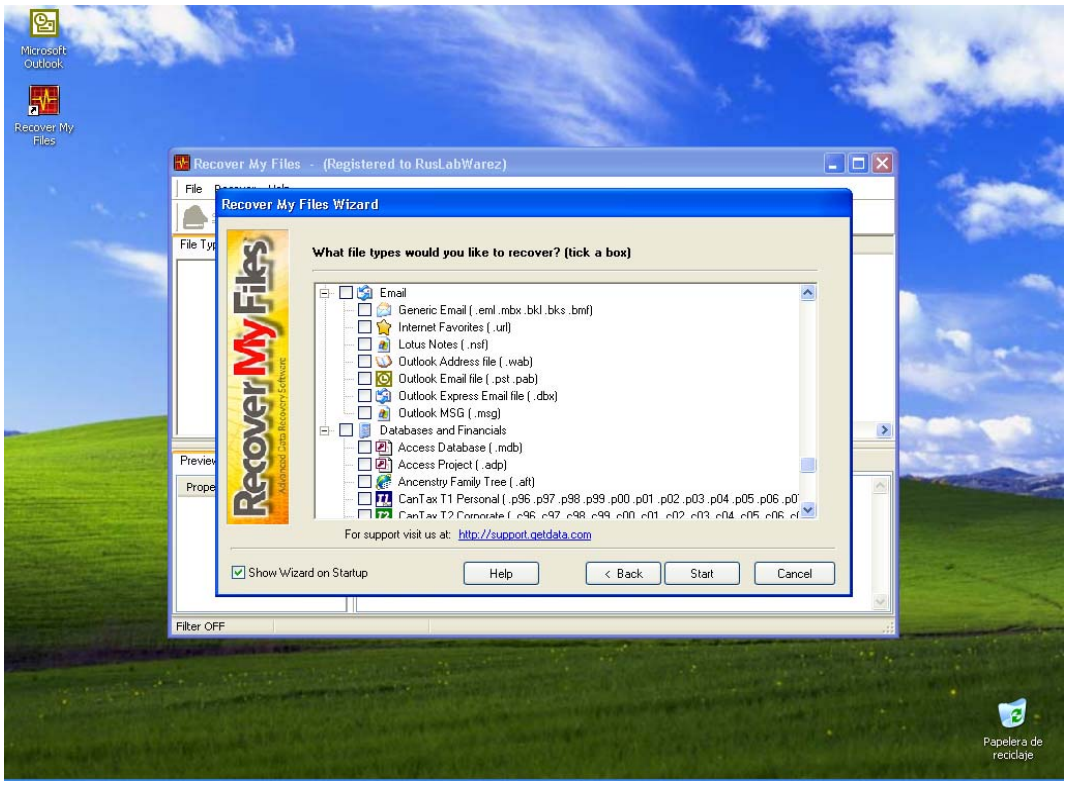
En las siguientes 6 imágenes se presenta los tipos de archivos que podemos recuperar con este programa, obsérvelos.

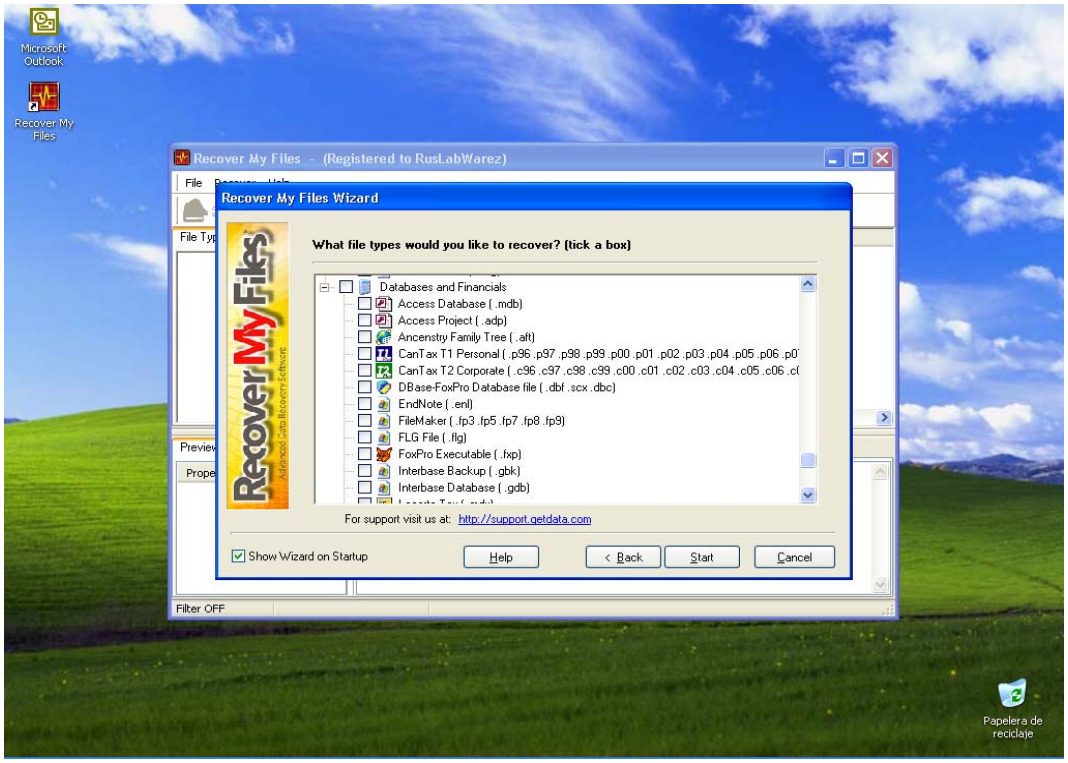

Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
Graphics
3d Studio Max (.max)
Adobe Indesign file (.indd)
Adobe Photoshop (.psd)
AutoCAD Drawing file (.dwg)
AutoCad DX File (.dxf)
AutoSketch (.skf)
Bentley Microstation v7 Drawing (.dgn)
Bentley MicroStation v8 Drawing (.dgn)
Bitmap (.bmp)
Canon Raw graphics file (.crw)
COREL Draw file (.cdr)
DesignCAD file (.dcd)
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje


Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
XARA Graphic file (.xar)
Documents
Adobe PageMaker (.pmd .p65)
Adobe Premier Project (.ppj)
Avery DesignPro (.zdp)
Casio Disk Title (.ctw)
CoolPage (.cpg)
Corel Presentation File (.shw)
Crystal Reports (.rpt)
Diablo2 Save (.d2s)
Etax file (.efx)
Family TreeMaker (.ftw)
FamilySearch file (.paf)
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje

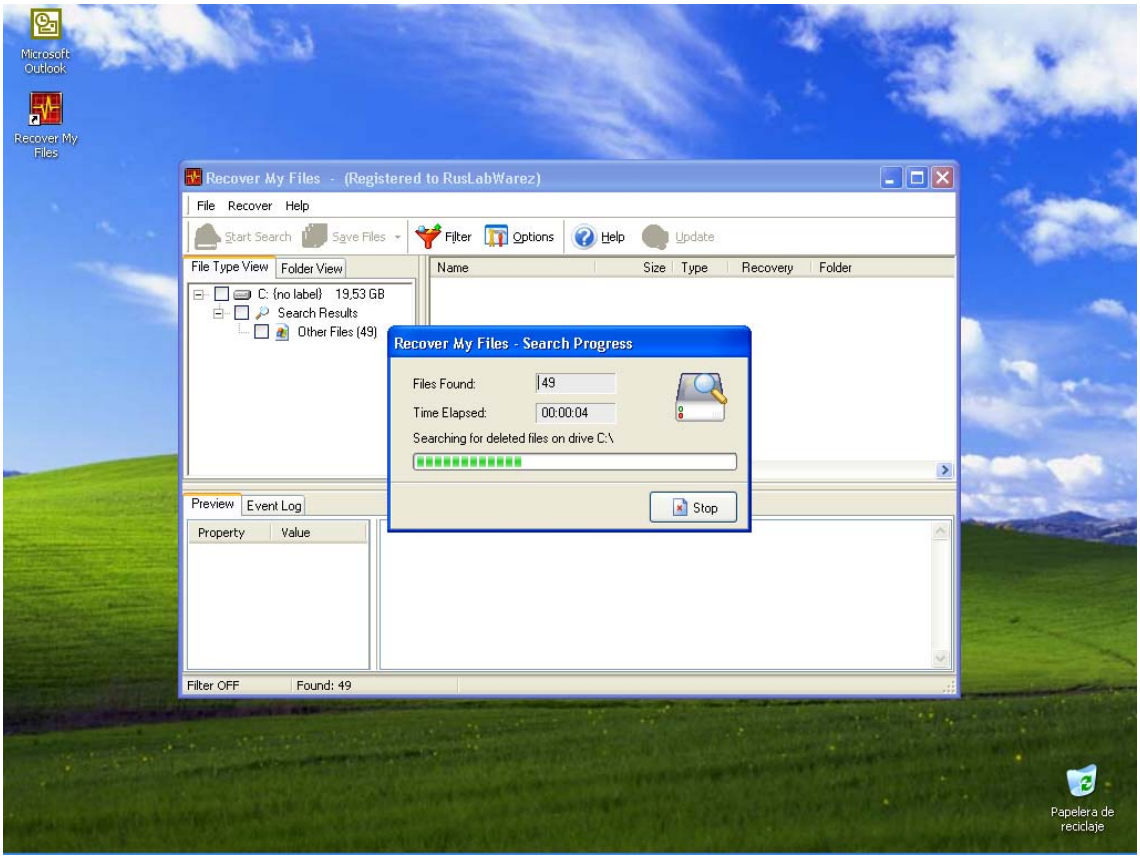

Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
XML Documents (.xml .xsl .svg .xms)
Archives
Cabinet compression file (.cab)
GZIP compression file (.gz .gzip)
LZH compression file (.lzh)
Miliki Super Compression (.qcf)
MS Backup File (.bkf)
RAR compression file (.rar)
Restrospect File (.rfb .rdb)
TAR archive file (.tar)
Zip compression file (.zip .jar .afz)
Multimedia
3GPP Multimedia file (Quicktime) (.3gp .3g2 .3gpp .3gp2 .mp4)
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje


Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
Multimedia
3GPP Multimedia file (Quicktime) (.3gp .3g2 .3gpp .3gp2 .mp4)
Adaptive MultiRate Audio (.amr)
ASF,WMA,WMV Multimedia file (.asf .wma .wmv .asx)
Audio Interchange file (.aif .aiff)
AVI Multimedia file (.avi)
CakeWalk Pro (.cwp)
Digital Speech File (.dss)
Digital Voice File (.dvf)
Finale Music file (.mus .fan)
Flash (.fla)
Fruity Loops file (.flp)
iTunes audio file (.m4a .m4b .m4p)
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje


Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
Email
Generic Email (.eml .mbx .bkl .bks .bmf)
Internet Favorites (.url)
Lotus Notes (.nsf)
Outlook Address file (.wab)
Outlook Email file (.pst .pab)
Outlook Express Email file (.dbx)
Outlook MSG (.msg)
Databases and Financials
Access Database (.mdb)
Access Project (.adp)
Ancenstry Family Tree (.aft)
CanTax T1 Personal (.p96 .p97 .p98 .p99 .p00 .p01 .p02 .p03 .p04 .p05 .p06 .p0
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje

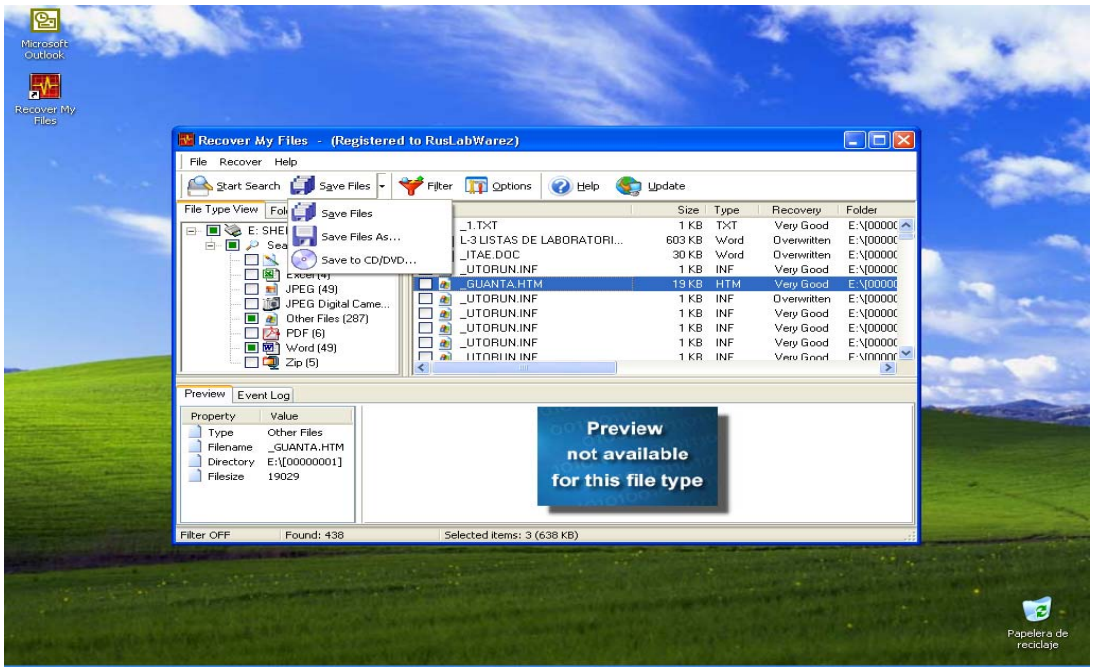

Microsoft Outlook
Recover My Files
Recover My Files - (Registered to RusLabWarez)
File
Recover My Files Wizard
What file types would you like to recover? (tick a box)
Databases and Financials
Access Database (.mdb)
Access Project (.adp)
Ancenstry Family Tree (.aft)
CanTax T1 Personal (.p96 .p97 .p98 .p99 .p00 .p01 .p02 .p03 .p04 .p05 .p06 .p0
CanTax T2 Corporate (.c96 .c97 .c98 .c99 .c00 .c01 .c02 .c03 .c04 .c05 .c06 .c
DBase-FoxPro Database file (.dbf .scx .dbc)
EndNote (.enl)
FileMaker (.fp3 .fp5 .fp7 .fp8 .fp9)
FLG File (.flg)
FoxPro Executable (.fxp)
Interbase Backup (.gbk)
Interbase Database (.gdb)
For support visit us at: http://support.getdata.com
Show Wizard on Startup
Help
< Back
Start
Cancel
Filter OFF
Papelera de reciclaje

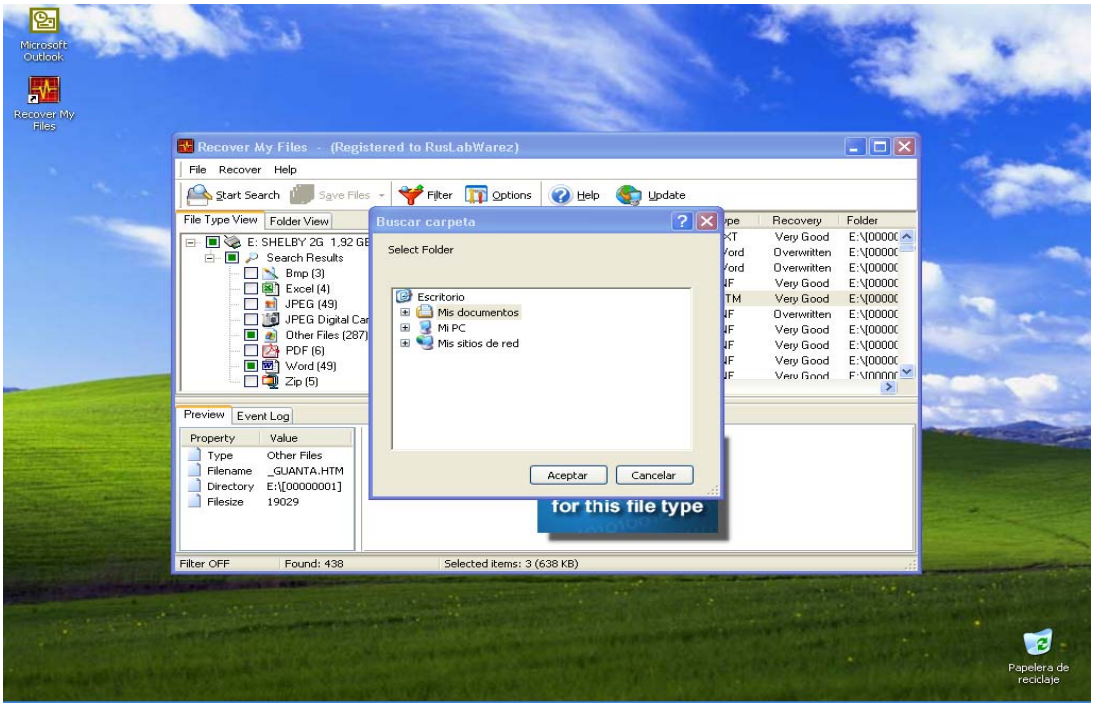
Como podemos ver el programa esta muy completo y fácil de utilizar, ya una vez seleccionados los tipos de archivos que se buscaran se observa el siguiente cuadro de dialogo que nos muestra el progreso de la búsqueda.



Una vez terminada la búsqueda nos indica cuantos archivos fueron encontrados con base en los que fueron señalados para la exploración inicial, de ahí podemos recuperar los que necesitamos, teniendo la posibilidad de una vista previa de los mismos.

Y para concluir con el proceso y tener acceso a los archivos buscados y encontrados, debemos guardarlos en una carpeta de nuestro equipo, CD o DVD para evitar nuevas pérdidas posteriores.





Tanto este como muchos otros programas dedicados a la recuperación de información en medios de almacenamiento masivo formateados son usados por dependencias de seguridad pública (en auditorias por ejemplo), así como por hacker´s para obtener información confidencial de las personas; con o sin autorización de ellas.

3.3 DESCRIPCIÓN DE LOS FALLOS EN UN DISCO DURO CON “DAÑO FÍSICO” Y TECNICAS DE RECUPERACIÓN POR LABORATORIOS ESPECIALIZADOS.

En este apartado se exponen los diferentes fallos a los que está expuesto un Disco Duro y el diagnostico correspondiente presentado por la empresa IT & DATA SERVICES para su reparación y recuperación de los datos.

Cabe mencionar que dada la alta seguridad de la empresa y la restricción al acceso a sus recursos tecnológicos para su operación, sólo se muestran imágenes permitidas por la misma para poder ejemplificar este tema.

Fallos en Cilindros de Ingeniería. (Diskware Failures).

Estos fallos son muy comunes en los dispositivos debido a una corrupción de los módulos de firmware en estas zonas.

El Firmware: es la información grabada durante el proceso de fabricación, indispensable para que el disco pueda inicializar y configurarlo además de acceder a los datos del usuario.

Aparte del micro código en el circuito impreso (PBC), la mayoría de unidades manejan, otra parte indispensable del micro código en el interior de la unidad, en unas zonas grabadas en los “platos” durante su fabricación.

El acceso a estas áreas requiere de una tecnología especializada, así como un amplio conocimiento de estas zonas; ya que el acceso a esos cilindros es de forma negativa – cyl, la mayoría de software que se puede encontrar para recuperar la información trabaja con cilindros en acceso positivo, así mismo una manipulación errónea podría inutilizar el disco para siempre, o dañarlo mucho más.

Un ejemplo de estos síntomas pueden aparecer cuando el disco no es detectado por el BIOS, se congela en el proceso, o lo detecta de manera errónea, Ej; detectado como en las familias Maxtor

“Discos Maxtor detectado como “Calypso, Ares 64k, Romulus, N40P, Nike, Athena,” etc”.

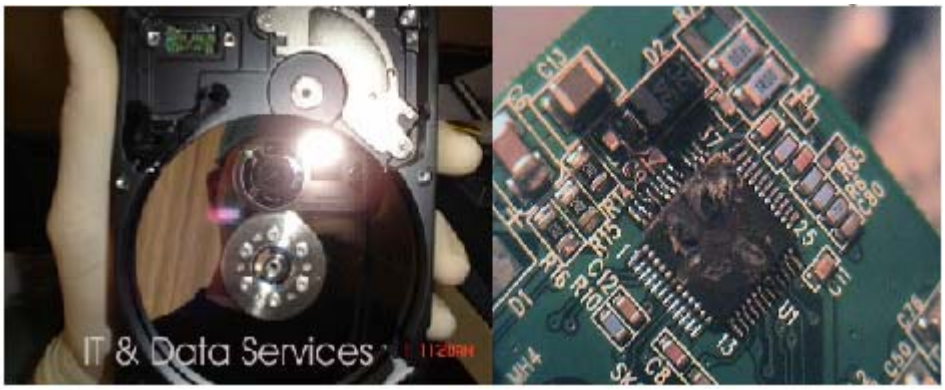
Fallos en el Sistema de Lectura/Escritura Read/Write System.

Pueden presentarse fallos en el sistema de lectura/escritura una manipulación incorrecta puede dañar, e incluso hacer imposible un intento posterior de recuperación. **Aparte que para abrir la unidad se requiere de un sistema controlado para el filtrado de partículas hasta del tamaño de 0.3 micras que puedan adherirse a la unidad o contaminar los sensores de las cabezas de lectura/escritura.**

Algunos síntomas se presentan como sonidos de golpes dentro de la unidad, aunque a veces puede tratarse de problemas en los cilindros de Ingeniería.

Fallos Mecánicos/Electrónicos. Mechanical/Electronic Problems.

Pueden presentarse como problemas desde el momento en que enciende la unidad como sonidos de golpes en el interior, o que la unidad no arranque completamente, un corto circuito, etc; aunque pudiera algunas veces confundirse con otros fallos, de ahí lo indispensable de **un adecuado diagnóstico** (Obsérvese la imagen)**.**



Fallos Lógicos.

Desde un simple formateo por error, un cierre incorrecto del sistema, virus, etc; son los causantes de la pérdida de datos a nivel lógico; aunque algunas veces los fallos de bajo nivel como los fallos en los módulos de ingeniería podría ocasionar también que se dañaran los datos a nivel lógico, pudiendo crear hasta una sobre escritura de los datos, de ahí la importancia de un diagnóstico eficaz y la ruta de acción adecuada para recuperar los datos.

Head Crash & Head Stiction.

Este tipo de situación puede presentarse en ciertos modelos de Discos Duros, generalmente de la línea de escritorio.

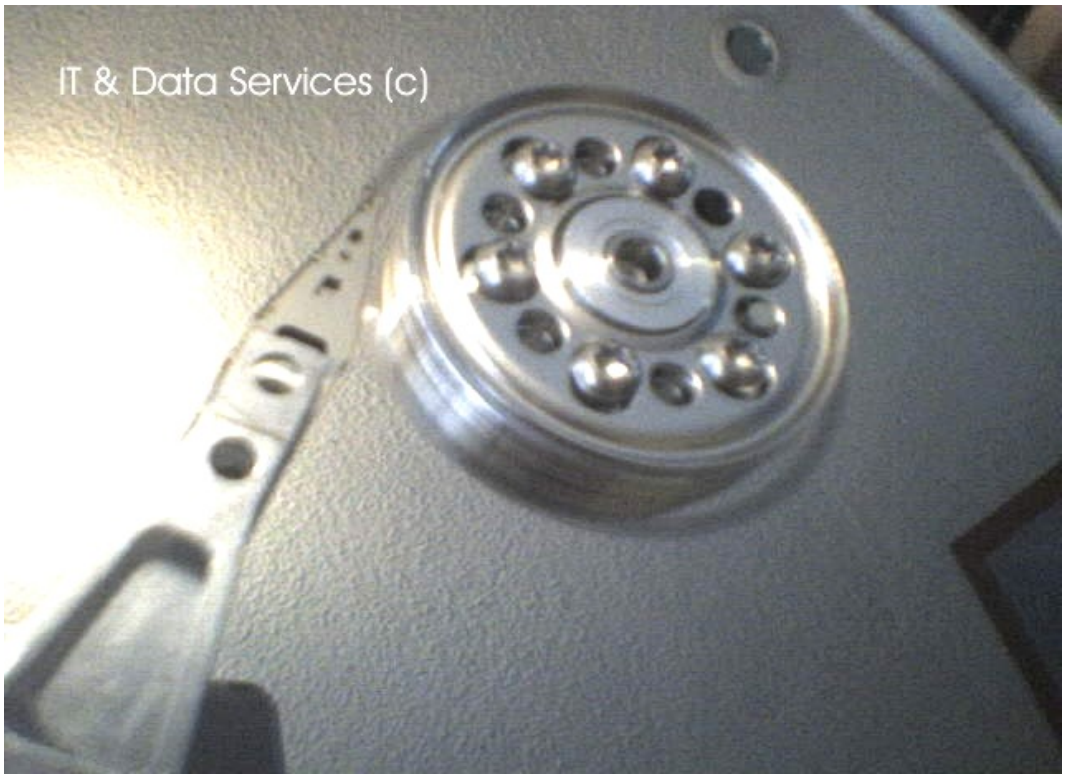
El término de Head Crash se denomina al hecho de que las cabezas de lectura/escritura por diversas situaciones (Contaminación de sensores MR, Pérdida de la Alineación, fallo en el Head Snack o Ensamble de Cabezas o hasta un intento de recuperación erróneo) aterrizan en la superficie del plato creando un surco desgastando el esmalte magnético que recubren los platos desde su fabricación.

Los síntomas visibles (Necesariamente en un cuarto limpio) se dan con la creación en la creación en la superficie de los platos de un desgaste o erosión de forma circular.

Head Stiction.

Se denomina el momento en que las cabezas R/W por diferentes situaciones se adhieren al plato, impidiendo el movimiento de este.

El intento de encender la unidad en esta situación dañaría mucho más el sistema de lectura/escritura así como podría crear una sobre tensión en el controlador de motor llegando a quemarlo.



Head Crash en un Disco Maxtor 9024DD2, los datos se pudieron recuperar exitosamente.

Servidores RAID.

En los servidores RAID, entre los Fallos más comunes aparte de los mencionados anteriormente, se encuentran:

- Fallos en la controladora RAID
- Pérdida de la configuración del Registro del Servidor
- Reconfiguración accidentalmente del Servidor
- Fallos en múltiples Discos.
- Reemplazo accidental de los componentes del medio.

Ante cualquier fallo mencionado anteriormente o los Fallos más comunes (Firmware, Fallos Mecánicos, Electrónicos, Head Crash) para minimizar el riesgo de dañar más la información posterior a la recuperación.
Recomendaciones:

- ✓ No reconfigure el arreglo
- ✓ No cambie el orden de los arreglos
- ✓ No corra herramientas de chequeo de disco como scandisk, defrag, Chkdsk.
- ✓ No acceda al sistema si uno o más de los discos comienzan a fallar.

Fallo en un Servidor Dell Power Edge 2800 RAID, 1.5 % de los datos se pudieron recuperar exitosamente.

Sectores Defectuosos Bad Sectors.

¿Porque no usar software que “repara” sectores para recuperar la información?

Lo que ocasiona que sien esa área se localizaba parte de la información de un archivo el contenido pueda perderse o parte del contenido sea sobrescrito por ceros.

Método para la recuperación de Sectores Defectuosos Bad Sectors.

Estos campos son grabados durante un formateo de bajo nivel, así como se inicializa los campos dedicados a los datos DATA (512 bytes), por lo que si se hace un LLF el campo de datos es rellenado con FF´s, bytes de testeo.

SERVO, GAP, ID, SYNC, DATA, ECC, GAP

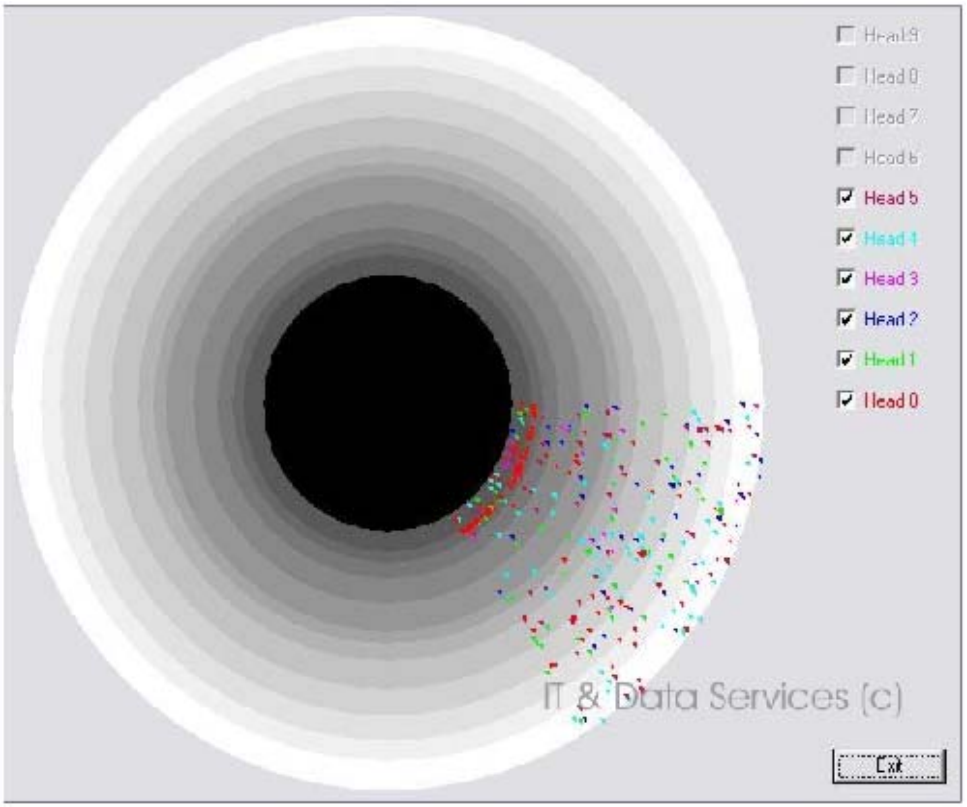
Cuando la unidad es programada para acceder a cierta zona del disco, las cabezas leen y checan los campos de CRC, antes de acceder al campo de DATA si dichos campos, no pueden ser leídos o su valor es incorrecto, el microprocesador informa al Host y es dado como sector dañado informando a los registros ATA, ya sea de tipo UNC; IDNF, etc., Lógicamente el campo de sector es marcado como BAD, sin embargo el acceso a este es posible, así como a los datos contenidos en el.

¿Como puede dañar más los datos e incluso el disco duro un intento de recuperación por software sin el control apropiado?

Los síntomas pueden empezar con “sectores defectuosos”.

En los casos que hemos visto, este tipo de falla puede ocurrir por varias situaciones una es debido a un daño, del sistema de archivos, o presencia de sectores dañados por lo que es muy importante que no se trate de recuperar con otros medios que no sean control por hardware y los algoritmos apropiados sobre todo que no lea ni escriba al disco pues es necesario localizar la falla, en algunas ocasiones se presentan **al apagarse mal el equipo** así también cuando el disco, es usado como servidor **“para atender solicitudes”** de I/O o por que se congela, en varios casos analizados se encuentra que se llega a sobrescribir parte de lo que es el sistema de archivos, por lo cual es importante no intentar acceder al disco para no hacerle más daño, y bajar el porcentaje de recuperación , en la

segunda causa, **“por sectores dañados”**, es necesario también no intentar “reparar sectores” con programas utilitarios como “HDD Regenerator” o cualquier otro, ya que este tipo de programas, cuando encuentran un sector defectuoso, lo tratan de leer y checar el CRC, una vez esto sin no concuerda, lo dan como “malo” y le escriben un patrón de bytes “FF” por lo que el contenido de ese sector pasa a ser llenado por este sector, **eliminando definitivamente el contenido anterior.**



Sistema de detección de fallos de sectores por cada cabeza de lectura/escritura

CONCLUSIONES

Ha quedado establecida la necesidad de analizar y normalizar los procesos para los Sistemas de Información con base en las Normas y Políticas actuales, ya que; esto es fundamental para el desarrollo de estos en un ambiente seguro y confiable. Así mismo, es indispensable trabajar con calidad y dedicación en los Sistemas de Información, puesto que; lo que se busca es la seguridad de la información, y por ende brindar confiabilidad y eficiencia a dichos sistemas.

Al concluir este trabajo destaca la importancia del desarrollar las etapas de los Sistemas de Información con apoyo, tanto en los documentos normativos oficiales vigentes, como en; los manuales respectivos de cada técnica y/o procedimiento ocupado, para lograr con esto cubrir satisfactoriamente los aspectos fundamentales en la administración de la información y poder minimizar los riesgos a los que están expuestos los datos con los que trabajamos cotidianamente.

Los objetivos particulares que se busca alcanzar en un Sistema de Información y principalmente en el manejo de la información son los siguientes:

- Calidad
- Seguridad
- Eficiencia

BIBLIOGRAFÍA:

Ford, James. “Quantum Cryptography Tutorial” Dartmouth College. 1996.

Langefors, Börje (1973). *Theoretical Analysis of Information Systems*. Auerbach.

Lomonaco, Samuel J. Jr. A Talk on Quantum Cryptography or How Alice Outwits Eve. 2001.

Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1998.

CIBERGRAFÍA

http://cibsi05.inf.utfsm.cl/presentaciones/empresas/Neosecure.pdf 19/05/08

http://elvex.ugr.es/decsai/java/pdf/2C-Datos.pdf

http://ftp.ucv.ve/Documentos/Congreso2008/Ponencias%20Martes%20110308/05.%20doc_iso27000_all.pdf 19/05/08

http://personales.ciudad.com.ar/roble/seguridadinformatica.htm

http://sociedaddelainformacion.wordpress.com/2007/02/25/la-familia-de-normas-isoiec-27000/ 19/05/08

http://www.27005.net/

http://www.aecirujanos.es/secciones/gestiondecalidad/cap4.pdf

http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/

http://www.iso.org

http://www.iso27000.es/doc_iso27000_all.htm 05/05/08

http://www.ISO27001security.com

http://www.ita.com.ar/winxp/

http://www.itson.mx/dii/jgaxiola/sistemas/introduccion.html#conceptos 10/09/08

http://www.itson.mx/dii/jgaxiola/sistemas/introduccion.html#conceptos 10/09/08

http://www.proyectosalonhogar.com/Enciclopedia/NE_etica.htm

http://www.security.kirion.net/seguridad/

ISO27001security forum

GLOSARIO:

AIA:

Federación Internacional Del Nacional Que Estandariza Asociaciones.

AEA:

Advanced Encryption Algorithm.

AES:

Advanced Encryption Standard.

ATA:

Serial ATA o S-ATA (acrónimo de *Serial Advanced Technology Attachment*) es una interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento, como puede ser el disco duro, u otros dispositivos de altas prestaciones que están siendo todavía desarrollados

BSI:

British Standards Institution la organización británica equivalente a AENOR en España.

CBC:

Cipher Block Chiang.

CFB:

Cipher feed back.

CRIPTOGRAFÍA:

(Kriptos=ocultar, graphos=escritura) la técnica de transformar un mensaje inteligible, denominado texto en claro, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos criptograma o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina algoritmo de encriptación.

DAS:

Direct Attached Storage.

DES:

Data Encription Estándar.

DATO:

Es la representación formal de hechos, conceptos o instrucciones adecuada para su comunicación, interpretación y procesamiento por seres humanos o medios automáticos.

FAT:

Tabla de asignación de archivos.

GATEWAY:

También llamados traductores de protocolos, son equipos que se encargan, como su nombre indica, a servir de intermediario entre los distintos protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí.

Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y, paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida.

HBAs:

Los adaptadores iSCSI host bus (HBAs) son tarjetas de red que incorporan un motor con la capacidad de proceso iSCSI integrada. Los HBAs iSCSI son tratados por el sistema operativo como controladores SCSI convencionales. En estos casos, el HBA no formará parte de la pila de red del sistema.

IEC:

International Electrotechnical Comisión.

IDEA:

International Data Encription Algorithm.

INFORMACIÓN:

En sentido general, la **información** es un conjunto organizado de datos **procesados**, que constituyen un mensaje sobre un determinado ente o fenómeno.

INTELIGENCIA:

Del latín *intellegentĭa,* es la capacidad de entender, asimilar, elaborar información y utilizarla adecuadamente. Es la capacidad de procesar

información y está íntimamente ligada a otras funciones mentales como la percepción, o capacidad de recibir dicha información, y la memoria, o capacidad de almacenarla

iSCSI:

Internet o los pequeños Interfaz de Sistemas de Computación. iSCSI es la transmisión de comandos SCSI y datos sobre redes IP.

ISL:

Inter Switch Link, enlace entre conmutadores.

ISO:

International Organization for Standardization.

ITU:

Unión Internacional de Telecomunicaciones.

LAN:

Red de Área Local (Local Area Network): es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de hasta 200 metros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

LUN:

Logical Unit Number.

MAINFRAMES:

Es un ordenador de grandes dimensiones pensado principalmente para el tratamiento de grandísimos volúmenes de datos. Se utiliza para aplicaciones de Banca, Hacienda y mercado de valores, aerolíneas y tráfico aéreo, así como de centro neurálgico de grandes empresas con un volumen de facturación elevado. En definitiva, es un ordenador grande, en todos los sentidos (tanto por su capacidad, como por el volumen que ocupa).

MAN:

Red de Área Metropolitana (Metropolitan Area Network): es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante

la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades que van desde los 2Mbps y los 155Mbps.

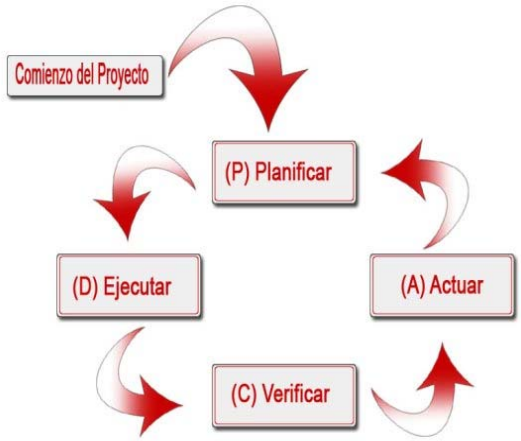
MTBF:

Tiempo Medio Entre Fallos.

MODELO PDCA:

El modelo en el que se basa el SGSI es denominado Modelo PDCA ("Plan-Do-Check-Act") que se representa en la siguiente figura:

Modelo PDCA



NAS:

Network Attached Storage. es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

NFS:

Network File System.

NTFS:

Nueva Tecnología de Sistema de Archivos.

OCDE:

Organización para la Cooperación y el Desarrollo Económico (Organisation for Economic Co-operation and Development).

OHSAS:

Sistemas de Gestión de Salud y Seguridad Laboral (*Occupational Health and Safety Management Systems*) son una serie de normas sobre la salud y seguridad en el trabajo.

PTR:

Plan de Tratamiento de Riesgos.

PYMES:

Pequeñas y Medianas Empresas.

RAID:

Originalmente del inglés *Redundant Array of Inexpensive Disks*, ·"onjunto redundante de discos baratos", en la actualidad también de *Redundant Array of Independent Disks*, "conjunto redundante de discos independientes".

RUTER:

Ruteador o encaminador es un dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos

SAN:

Red De Área De Almacenamiento (Storage Area Network).

SATA:

Aparte de las más comunes Universal Serial Bus (USB) y FireWire 400, otro interfaz externa utilizados en la transferencia de datos es eSATA. Simplemente significa eSATA externo de serie Adjunto de Tecnología Avanzada.

SCSI:

SCSI (Pequeño Computer System Interface) es un conjunto de normas ANSI para conectar dispositivos a los sistemas informáticos. La gran mayoría de los dispositivos SCSI son dispositivos de almacenamiento de datos.

SGSI:

Sistema de Gestión De La Seguridad De La Información.

SHOULDER SURFING:

Esta técnica es la más básica y consiste en merodear a aquellas personas que conocen el password que se quiere averiguar intentando ver si se consigue visualizar el momento en que el password es tipeado en un teclado o escrito en algún papel, variantes más modernas de esta técnica incluyen programas residentes que monitorean las teclas que se oprimen en el teclado, cámaras que registran lo que se tipea desde un punto elevado, etc.

SWITCH:

En castellano "conmutador": es un dispositivo analógico de lógica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TECNOLOGÍA:

Es el conjunto de habilidades que permiten construir objetos y máquinas para adaptar el medio y satisfacer nuestras necesidades. Es una palabra de origen griego, τεχνολογος, formada por *tekne* (τεχνη, "arte, técnica u oficio") y *logos* (λογος, "conjunto de saberes").

Aunque hay muchas tecnologías muy diferentes entre sí, es frecuente usar el término en singular para referirse a una cualquiera de ellas o al conjunto de todas. Cuando se lo escribe con mayúscula, tecnología puede referirse tanto a la disciplina teórica que estudia los saberes comunes a todas las tecnologías, como a educación tecnológica, la disciplina escolar abocada a la familiarización con las tecnologías más importantes.

TELECOMUNICACIONES:

Del prefijo griego *tele*, "distancia" o "lejos", "comunicación a distancia": es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término *telecomunicación* cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores a nivel de enlace. El Día Mundial de la Telecomunicación se celebra el 17 de mayo.

TELETRABAJO:

Literalmente trabajo a distancia, se refiere al desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual. Suele referirse a trabajos de oficina que precisan de una interacción mínima con el cliente y que no requieren de presencialidad. Es habitual el uso de medios informáticos para comunicarse con los clientes o compañeros de trabajo, para el envío de resultados y, en la mayoría de los casos, para la realización de la actividad.

TI:

Tecnología de la información.

UNSCC:

Comité De Coordinación De Los Estándares De Naciones Unidas.

VPN:

Red virtual Privada (Network Virtual Private): es una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

WAN:

Red de Área Extensa (Wide Area Network). WAN es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel planetario

WWN:

World Wide Name: o AON, es uno de 64 bits utilizados en la dirección de canal de fibra de redes para identificar cada uno de los elementos en una red de canal de fibra.

ANEXO

ARTÍCULOS DE LA NORMA ISO/IEC27001 APLICADOS A NUESTRO ESTUDIO.

A.1 INTRODUCCIÓN.

Con el objeto de brindar seguridad, confiabilidad y calidad, en los Sistemas de Información se han creado normas que regulan el manejo de la información con estándares nacionales e internacionales (como es el caso de ISO), para evitar daños colaterales en dichos sistemas.

Para esto, cada propuesta de normalización es presentada ante los organismos competentes en el área que será aplicada para la valoración, modificación y aceptación, siendo (en el caso de México) presentada para el conocimiento del público en el Diario Oficial de la Federación.

Es necesario aclarar que las normas publicadas en determinado caso son única y exclusivamente para el proyecto que fue destinado, y en determinado lapso de tiempo estas pueden volverse obsoletas si llegase a existir alguna propuesta de modificación en alguno de sus artículos y deberá acatarse la norma de tipo oficial que se encuentre vigente.

Así mismo, cabe destacar que este tipo de normas manejan todas las posibles fallas con las que se puede encontrar el usuario, ya que en determinadas situaciones es imposible cumplirse al pie de la letra lo que establecen y por tal motivo se contemplan excepciones que amplían las posibilidades de ser implementadas y facilitan el manejo de éstas.

Las empresas y/o industrias dentro de sus procesos internos deberán considerar qué tipo de norma aplica al bien o servicio que ofrecen, siendo sometidos a auditorias de calidad y seguridad, con previo aviso de las autoridades, puesto que; lo que se busca con la normalización de los procesos de producción es generar bienes y servicios de calidad.

A2. NORMA ISO/IEC SERIE 27000 APLICADA A NUESTRO ESTUDIO.

La siguiente tabla muestra los artículos en los que se basa nuestro estudio, que son extracto de la serie de normas ISO/IEC 27000, con su debida referencia:

Ref.	Objetivo	Consejos de implementación	Posibles métricas
4. Evaluación y tratamiento de riesgos			
4.1	Evaluación de riesgos de seguridad	*Se puede usar cualquier método de gestión de riesgos de seguridad de la información, con preferencia por métodos documentados, estructurados y generalmente aceptados como OCTAVE, MEHARI, ISO TR 13335 ó BS 7799 Parte 3 (y, en su momento, ISO/IEC 27005).*	Porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".
4.2	Tratamiento de riesgos de seguridad	*La gerencia (específicamente, los propietarios de activos de información) necesita evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones deben documentarse en un Plan de Tratamiento de Riesgos (PTR). Es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información que se estiman dentro de la "tolerancia al riesgo" de la organización, sin que sea éste el enfoque por defecto.*	Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia. Costes de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI. Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios.

5. Política de seguridad			
5.1	Política de seguridad de la información	*Piense en términos de un manual o wiki de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.*	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoria, gerencia o auto- evaluación).
6. Aspectos organizativos de la seguridad de la información			
6.1	Organización interna	*Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y Compliance.*	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.
6.2	Terceros	*Haga inventario de conexiones de red y flujos de información significativos con 3as partes, evalúe sus riesgos y revise los controles de seguridad de*	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

		información existentes respecto a los requisitos. ¡Esto puede dar miedo, pero es 100% necesario! *Considere exigir certificados en ISO/IEC 27001 a los partners más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.*	
7. Gestión de activos			
7.1	Responsabilidad sobre los activos	*Elabore y mantenga un inventario de activos de información (similar al preparado en su día para el Efecto 2000), mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. Ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.).* *Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.*	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables.
7.2	Clasificación de la	*¡Mantenga la sencillez! Distinga los*	Porcentaje de activos de información en cada

	información	*requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo.* *Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad.*	categoría de clasificación (incluida la de "aún sin clasificar").
8. Seguridad ligada a los recursos humanos			
8.1	Antes de la contratación	*Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.*	Porcentaje de nuevos empleados o *pseudo-empleados* (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.
8.2	Durante la contratación	*La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va*	Respuesta a las actividades de concienciación en seguridad medidas por, p. Ej., el número de e-mails y llamadas relativas a iniciativas de concienciación

		a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc. *Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.*	individuales.
8.3	Cese o cambio de puesto de trabajo	*Véase Sección 7.1. La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente.* *Examine qué accesos necesita revocar en primer lugar cuando un empleado presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables?* *Haga un seguimiento del uso del e-*	Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

		mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).	
9. Seguridad física y ambiental			
9.1	Áreas seguras	*El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. Ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI).* *Examine la entrada y salida de personas a/de su organización.* *¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. Ej.,*	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

		azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo). *Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.*	
9.2	Seguridad de los equipos	*Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita. Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores,*	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

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

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

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

		físico sino electrónico (a través de las redes). *Encripte todos los datos sensibles o valiosos antes de ser transportados.*	
10.8	Intercambio de información	*Estudie canales de comunicaciones alternativos y "preautorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.*	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.
10.9	Servicios de comercio electrónico	*Trabaje estrechamente con las unidades de negocio para desarrollar un eBusiness seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de eCommerce, desde el principio (también en cualquier cambio/actualización posterior). Insista en el valor añadido de la seguridad en la reducción de riesgos comerciales, legales y operativos asociados al eBusiness. Trabaje los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad.*	"Estado de la eSeguridad", es decir, un informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas, cambios planificados, etc.
10.10	Supervisión	*El viejo axioma del aseguramiento de la calidad "no puedes controlar*	Porcentaje de sistemas cuyos *logs* de seguridad (a)

		lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico. Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.	están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de *logs* y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los *logs* de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.
11. Control de accesos			
11.1	Requisitos de negocio para el control de accesos	*Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.*	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.
11.2	Gestión de acceso de usuario	*Cree la función diferenciada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la*	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes").

		dirección de seguridad de la información. Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible.	
11.3	Responsabilidades del usuario	*Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio.* *Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.*	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) Totalmente documentadas y (b) formalmente aceptadas.
11.4	Control de acceso a la red	*Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en*	Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en

		profundidad)	insignificantes/preocupantes/críticos).
11.5	Control de acceso al sistema operativo	*Implante estándares de seguridad básica para todas las plataformas informáticas y de comunicaciones, recogiendo las mejores prácticas de CIS, NIST, fabricantes de sistemas, etc.*	Estadísticas de vulnerabilidad de sistemas y redes, como nº de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias).
11.6	Control de acceso a la aplicación y a la información	*Implante estándares de seguridad básica para todas las aplicaciones y middleware, recogiendo las mejores prácticas y checklists de CIS, NIST, fabricantes de software, etc.*	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)".
11.7	Ordenadores portátiles y teletrabajo	*Tenga políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware. Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como*	"Estado de la seguridad en entorno portátil / teletrabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (*laptops*, PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, *firewalls* personales, etc.

		antivirus, parches, actualizaciones, software cortafuegos, etc.	
12. Adquisición, desarrollo y mantenimiento de los sistemas de información			
12.1	Requisitos de seguridad de los sistemas de información	*Involucre a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan. Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien.* *Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas. Numerosas referencias ofrecen orientación sobre la implementación, como, p. ej., OWASP.*	Ver 11.1
12.2	Procesamiento correcto en las aplicaciones	*Siempre que sea posible, utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc.* *Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control).*	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.

		Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc.	
12.3	Controles criptográficos	*Utilice estándares formales actuales tales como AES, en lugar de algoritmos de cosecha propia. ¡La implementación es crucial!*	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses).
12.4	Seguridad de los archivos de sistema	*Aplique consistentemente estándares de seguridad básica, asegurando que se siguen las recomendaciones de CIS, NIST, fabricantes de sistemas, etc.*	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares.
12.5	Seguridad en los procesos de desarrollo y soporte	*Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.* *Trate el desarrollo e implementación de software como un proceso de cambio. Integre las*	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

		mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).	
12.6	Gestión de la vulnerabilidad técnica	*Haga un seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update o Secunia Software Inspector). Evalúe la relevancia y criticidad o urgencia de los parches en su entorno tecnológico.* *Pruebe y aplique los parches críticos, o tome otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente. Evite quedarse tan atrás en la rutina de actualización de versiones que sus sistema queden fuera de soporte por el fabricante.*	Latencia de parcheo o semiperiodo de despliegue (tiempo que ha llevado parchear la mitad de los sistemas vulnerables -evita variaciones circunstanciales debidas a retrasos en unos pocos sistemas, tales como portátiles fuera de la empresa o almacenados-).
13. Gestión de incidentes en la seguridad de la información			
13.1	Notificación de eventos y puntos	*Establezca y dé a conocer una hotline (generalmente, el helpdesk*	Estadísticas del *helpdesk* de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad

	débiles de la seguridad de la información	*habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad.*	de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.
13.2	Gestión de incidentes de seguridad de la información y mejoras	*Las revisiones post-incidente y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.*	Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida. Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.
14. Gestión de la continuidad del negocio			
14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	*Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.).* *Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio.*	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante tests apropiados en los últimos 12 meses.

		Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre. *Obtenga consejos de implantación en BS 25999 - Gestión de la Continuidad de Negocio.*	
15. Cumplimiento			
15.1	Cumplimiento de los requisitos legales	*Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.*	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	*Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen*	Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.

		funcionamiento.	
15.3	Consideraciones de las auditorías de los sistemas de información	*Invierta en auditoría TI cualificada que utilice ISO 27001, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación.* *Examine ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental" como fuente valiosa para la realización de auditorías internas del SGSI. ISO 19011 proporciona un marco excelente para crear un programa de auditorías internas y contiene asimismo las cualificaciones del equipo de auditoría interna.*	Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.