Universidad
Carlos III de Madrid

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA
EN INFORMÁTICA DE GESTIÓN

CONTROLES Y AUDITORÍA EN REDES DE DATOS. GUÍA PRÁCTICA.

DICIEMBRE 2010

Autora: Ángeles Tapiador Sanz. NIA: 100053016

Tutor: Miguel Ángel Ramos González.

Título: CONTROLES Y AUDITORÍA EN REDES DE DATOS. GUÍA PRÁCTICA.

Autor: ÁNGELES TAPIADOR SANZ.

Director: MIGUEL ÁNGEL RAMOS GONZALEZ

EL TRIBUNAL

Presidente: AGUSTÍN ORFILA DÍAZ-PABÓN

Vocal: JESÚS M. GAGO MEJÍAS

Secretario: JOSÉ MONTERO CASTILLO

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 17 de Diciembre de 2010 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

Hace ya unos pocos años que empecé la Universidad. Primeramente y un poco perdida empecé la diplomatura en estadística, y al año siguiente se me brindó la oportunidad de empezar la carrera que ahora termino. Sabía que me costaría y que tendría que esforzarme pero a pesar de ello para mí era una gran ilusión que pudiera decirme a mí misma que lo había conseguido, que pudiera decir que había conseguido ser ingeniero, técnico en este caso. Cuando empecé esta carrera tuve el mayor apoyo que podía tener por parte de mi madre, que desde el primer día confió en mí, y que sabía que si me lo propondría lo conseguiría. Recuerdo que el verano antes de empezar la carrera lo hablábamos en el balcón de mi casa y que desde el primer día me apoyó y sigue haciéndolo siempre como la que más. A ella va dedicado este proyecto.

Por otra parte, una vez empecé la carrera me vino otro gran apoyo, que también me convenció para hacer esta carrera antes de empezar. El que antes de empezar la carrera era mi amigo, y que se puede decir que nada más empezarla se convirtió en mi novio, y el que poco antes de acabarla ya era y es mi marido. Con él han sido muchas las horas de tener que aguantarme con prácticas para arriba y para abajo, y el que sin duda me enseñó que con esfuerzo todo se saca. A él también va dedicado este proyecto.

Y finalmente no puedo dejar de mencionar a las dos personas que más me han dicho toda la vida: “estudia, estudia”, y que han sido y son de lo más importante para mí. Mis abuelos, Félix y Ángela. Ellos me han enseñado otras cosas que no se aprenden en la carrera pero que son las mejores lecciones de vida. A ellos también les dedico este proyecto.

Y ya para terminar, pues también le doy las gracias a mi hermano y mi padre ¡que también me han estado soportando muchos años de carrera!

MIL GRACIAS A TODOS, ¡SOIS LO MEJOR QUE TENGO!

ÍNDICE

Este proyecto está dividido en varias partes, pero la parte central se basa en los distintos controles de la ISO 27002 aplicables para la empresa para comprobar en qué estado se encuentran las redes de datos, ya sea por conocimiento interno o por vistas a una futura certificación. Cabe decir que la ISO 27002 no es certificable, esta ISO trata los distintos controles y buenas prácticas aplicables a la empresa y que serán una parte para el cumplimiento de la ISO 27001 que en este caso sí es certificable.

Durante el proyecto hay una primera parte que comenta un poco el tema de redes de datos, es un englobe general del tema. A continuación se trata el tema de la auditoría con información sobre todo de la web de ISACA.

La parte central del proyecto son los siguientes puntos que son la elaboración de la guía aplicable a las redes de datos de la empresa. Consiste en filtrar los controles de la ISO 27002 aplicables a las redes. De estos controles se comenta un poco de cada uno para conocer sobre que tratan y en qué consisten.

Una vez tenemos los puntos localizados podemos pasar a la aplicación que se ha codificado sobre Delphi. Dicha aplicación consta de veintidós preguntas que son verificaciones sobre dichos controles y se pueden valorar de uno a cinco. Dependiendo de los resultados podremos valorar en qué estado se encuentra nuestro sistema de cara a una auditoría.

CAPÍTULO I
INTRODUCCIÓN

OBJETIVO

El objetivo de este proyecto ha sido la elaboración de una guía actualizada para realizar una auditoría a los sistemas de Comunicación y Redes de una empresa. Para ello se han seguido las directrices marcadas por la ISO/IEC 27002: 2005.

Además de las directrices marcadas por la ISO se han llevado a cabo ciertas comparativas en los puntos procedentes de la guía relacionándolos con COBIT e ITIL.

No todos los puntos de esta ISO son acerca de sistemas de redes por lo que se ha procedido a filtrar aquellos puntos que están más relacionados sobre el tema.

Con estos puntos se ha redactado una propuesta para aplicar una auditoría a una empresa en el ámbito específico de las redes de comunicaciones.

Una vez elaborada la guía se ha procedido a la elaboración de un cuestionario el cual es una aplicación en el que se pregunta acerca de los puntos ya filtrados de la ISO para hacer más cómoda la labor del auditor.

Dicho cuestionario está formado por veintidós preguntas de índole sencilla en la que a través de las respuestas de las mismas se podrá saber si la auditoría ha pasado con éxito o no. Además la aplicación tendrá la posibilidad de configurar los pesos de las preguntas pudiéndolas adaptar así al ejercicio que ejerza cada empresa.

IMPORTANCIA DEL TEMA

En evidente la importancia que tiene este tema para la seguridad de cualquier empresa. Sea cual sea el ejercicio al que se dedique una empresa ésta va a trabajar con datos.
Los datos son la esencia de cualquier empresa, es lo que la mueve. Es por ello que la importancia de los mismos se manifiesta de una manera evidente.

Los datos hay que tratarlos teniendo en cuenta la LOPD y todo lo que ello conlleva, a lo largo de este proyecto se cuenta la importancia de las política de seguridad de la empresa o cosas que a simple vista pueden parecer prescindibles pero que en la práctica son vitales.

Las copias de respaldo de los datos son esenciales, imaginemos que pasa cualquier altercado en la empresa y perdemos todos los datos. Esa empresa estaría perdida.
Cosas que pueden parecer menos importantes podrían ser por ejemplo el tener debidamente protegidos los cables de un CPD o debidamente etiquetados. En la actualidad muchas empresas no etiquetan los cables. El no hacerlo conlleva problemas en el futuro. No hay que olvidar que un trabajo tan sencillo como etiquetar un cable nos puede evitar muchos problemas futuros.
Otro ejemplo podría ser equipos que no estén debidamente ventilados, podríamos perder el equipo, y si hablamos de un servidor podría provocar la parada de una parte de la empresa.

Todos estos problemas como comentaba anteriormente tienen solución, y esta solución es poner medios antes de que ocurran las cosas, con el trabajo de todos, poco trabajo, podemos ayudar a que en el futuro no tengamos otros problemas mayores, que ya no tengan solución y que puedan llevar a tener grandes pérdidas a la empresa.

ESTRUCTURA

La composición de este proyecto se divide de la siguiente manera:
INTRODUCCIÓN: Dentro de ésta los objetivos de este proyecto fin de carrera y la importancia del tema.
Después tenemos una parte de INTRODUCCIÓN A LAS REDES, en esta parte se puede ver todo lo relacionados con las redes, componentes y algunos conceptos que se usan a lo largo de este proyecto.
Seguidamente tenemos el punto de INTRODUCCIÓN A LA AUDITORÍA, en este punto se explican los conceptos relacionados con la auditoría, algunos tipos, y todo esto relacionado y explicado con información de la Web de ISACA.
A continuación tenemos la GUÍA sobre la ISO/IEC 27002 2005. En esta guía se filtran los puntos relacionados con las redes y las comunicaciones, los puntos que se han filtrado son los siguientes:

PUNTO 5: POLÍTICA DE SEGURIDAD. (5.1).
PUNTO 9.2: SEGURIDAD DE LOS EQUIPOS. (9.2.1, 9.2.2, 9.2.3).
PUNTO 10.2: GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS.
PUNTO 10.6: GESTIÓN DE LA SEGURIDAD EN REDES.
PUNTO 11.4: CONTROL DE ACCESO A LA RED.
PUNTO 11.7: ORDENADORES PORTÁTILES Y TELETRABAJO.
PUNTO 12.3: CONTROLES CRIPTOGRÁFICOS.

Los puntos están con el texto original y a continuación comentados.
En los puntos que se han podido se ha relacionado con COBIT e ITIL.

Después de la guía y usando los puntos citados anteriormente se ha elaborado una APLICACIÓN para realizar una auditoría en una empresa. Ésta está comentada y explicada.

Después de todo esto que es el grueso de la aplicación tenemos las CONCLUSIONES, y los

OBJETIVOS CUMPLIDOS.

A continuación en los ANEXOS tenemos redactado y comentado el Título VIII del reglamento de Desarrollo de la LOPD. También podemos encontrar el CÓDIGO DE LA APLICACIÓN. Y un GLOSARIO con términos usados a lo largo de este proyecto.

Finalmente el proyecto termina con la BIBLIOGRAFÍA.

CAPÍTULO II
INTRODUCCIÓN A REDES

1. INTRODUCCIÓN

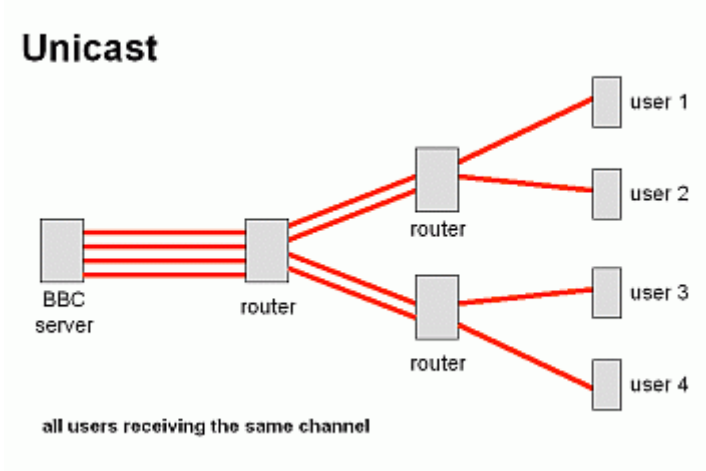
Si miramos en el diccionario de la Real Academia de la Lengua Española el significado de la palabra "red", encontramos lo siguiente: *Conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden intercambiar información.*

Esta definición es muy básica así que ampliaremos la información. Cuando hablamos de las redes en general nos podemos estar refiriendo a redes de voz, datos, y vídeo Así a groso modo, se puede definir la red de voz como la red telefónica, la de datos, como la red que usamos para poder conectarnos a Internet y la red de vídeo con la que podemos ver estos y descargárnoslos, *streaming* por ejemplo.

2. TIPOS DE ENLACES

Otros conceptos generales son los tipos de enlace existen, podemos hablar de varios tipos: enlaces directos, en los que emisor y receptor se comunican sin nodos intermedios. Los enlaces directos punto a punto en la que solo un emisor con un receptor comparten el mismo medio. Y enlaces directos de difusión: en los que hay más emisores compartiendo el mismo medio.

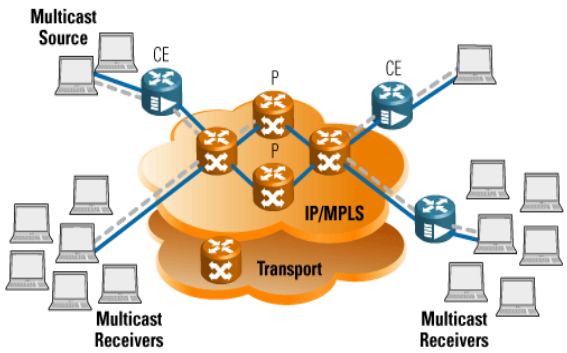
Los envíos de información a través de la red pueden ser *Unicast*, en los que tenemos n receptores definidos por el ancho de banda en los que la información se envía de uno en uno.



digitalradiotech.co.uk

Broadcast, que se da cuando el emisor envía un mensaje a todos los miembros de la subred incluyendo los receptores que están interesados en ese paquete como a los que no están interesados por él.

Y por último tenemos el *Multicast*, en este caso, el emisor envía una información solo a los receptores de la subred que estén interesado en esa información.



advanced.comms.agilent.com

Podemos clasificar las redes también según diversos criterios, por ejemplo según el diseño de la subred, en este caso podemos encontrar redes dedicadas como las punto a punto o las malladas, o Redes de difusión como las LAN.

3. OTRAS CLASIFICACIONES

También podemos clasificar las redes según el diseño de la subred. En este nivel podemos encontrar las redes de conmutación de paquetes, de mensajes o de circuitos.

3.1 REDES DE CONMUTACIÓN

3.1.1 DE CIRCUITOS

Las redes de **conmutación de circuitos** establecen un camino directo y dedicado entre el emisor y el receptor, y ésta se establece en tres fases, establecimiento de conexión, transferencia de información, y liberación del circuito.

Según:

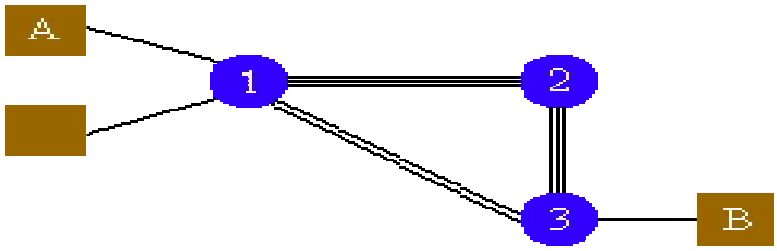
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1

Son el primer tipo de redes de conmutación inventadas. Se utilizan desde el invento de la central telefónica automática. En este tipo de red, se establece un camino directo y dedicado entre el equipo origen y el destino.

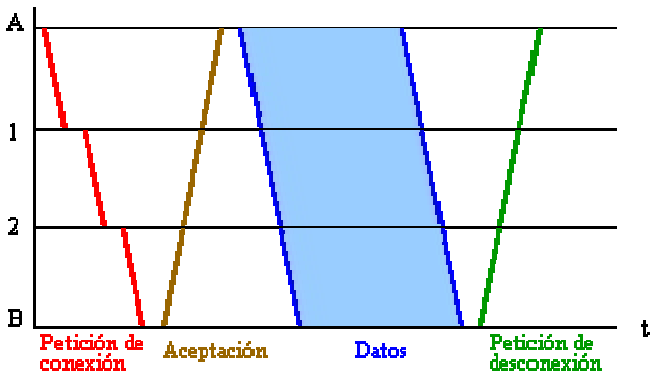
Transmisión de Datos.

El proceso de comunicación se lleva a cabo en tres fases:

1. *establecimiento de la conexión.*
2. *transferencia de información.*
3. *liberación de la conexión.*



Para comprenderlo mejor, se utiliza el siguiente ejemplo (ver imagen), siendo el equipo "A" el que se quiere conectar al "B", pasando la llamada a través de los nodos de conmutación "1" y "3".



Primero se establece la conexión. Para ello, el equipo origen solicita la conexión con el destino, mandando a tal efecto la dirección al nodo periférico. Este toma una decisión de encaminamiento, buscando el camino más rápido y cómodo. Se requieren dos caminos, uno de ida y otro de vuelta, que pasen ambos por los mismos nodos. Esta petición de conexión llega al siguiente nodo, que vuelve a decidir el mejor camino, así hasta llegar al destino, el cual contesta con una señal de aceptación, que vuelve a hacer el camino pero en sentido inverso.

La petición de conexión sufre un retardo en cada nodo por el que pasa debido a que estos deben tomar decisiones. Sin embargo, la señal de aceptación no sufre retardo alguno al haberse establecido el circuito anteriormente.

A continuación, con el circuito establecido y en exclusiva, los dos terminales pueden intercambiar información durante todo el tiempo que sea necesario. Dicha información no sufre retardo alguno.

Por último, cuando uno de los dos equipos desea finalizar la conexión (el destino, por ejemplo), se envía una señal de petición de desconexión. Al pasar ésta por cada nodo, estos cierran o liberan las conexiones entre entradas y salidas que establecen el circuito. Esta señal tampoco sufre retardo.

Transmisión de Datos.

El origen de este tipo de redes son las redes telefónicas. Hoy en día se utilizan para transmitir datos, pues incluso en la actualidad la red telefónica es digital. Otro ejemplo claro de red de conmutación de circuitos es la ISDN o RDSI (Red Digital de Servicios Integrados), que permite transmitir voz y datos.

El mecanismo de conmutación permite crear un circuito dedicado entre origen y destino, a través de los distintos nodos de la red. Este circuito es de uso exclusivo y durante tiempo ilimitado, hasta la petición de desconexión. En definitiva, equivale a poseer una línea privada entre origen y destino.

La otra gran ventaja de este tipo de redes estriba en la sencillez de la tecnología empleada, y además en que se posee gran experiencia en el uso de dicha tecnología.

Sin embargo, este tipo de red también posee sus inconvenientes. El principal es que el equipo origen y el equipo destino deben transmitir a la misma velocidad, pues si no, el sistema no funciona al no existir mecanismos de control de flujo. Por lo tanto, el sistema resulta muy poco flexible, ya que se debe transmitir continuamente, y además siempre con un flujo de datos constante, se tenga necesidad de transmitir o no. El sistema no acepta transmisión a ráfagas.

Otro inconveniente es el de saturación de la red que se congestiona si se realizan muchas llamadas, es decir, si muchos usuarios quieren conectarse a la vez. Esto se debe a que el número de canales disponibles es limitado, por lo que si todos ellos ya están siendo utilizados, ningún otro usuario puede conectarse, quedándose sin servicio. En compensación, los usuarios que sí están conectados, reciben siempre un servicio perfecto, independientemente del número de usuarios conectados.

3.1.2 REDES DE CONMUTACIÓN DE PAQUETES

Las redes de conmutación de paquetes se utilizan para enviar paquetes propiamente dichos, estos paquetes de información vienen divididos en los datos y en la información de control. Los datos es la información a enviar, y la información de control contiene la ruta a seguir hasta llegar al destino.

Usando esta técnica lograremos una mayor velocidad de transmisión puesto que además d ser conexiones más rápidas ya de por sí, se pueden seguir aceptando datos a pesar de que esto ralentice algo más el proceso. También podemos usar prioridades en los paquetes si requerimos de alguno con mayor rapidez que otro.

Para poder usar esta conmutación de paquetes, usamos los conocidos como datagramas y los circuitos virtuales. Los datagramas pueden estar orientados a conexión u orientados a no conexión, para ello se definen los protocolos TCP orientado a conexión y seguro, y UDP orientado a no conexión en la que no hay garantía de que los paquetes lleguen bien.

Por otra parte hablamos de los circuitos virtuales, estos tienen una funcionalidad similar a las redes de conmutación de circuitos. Antes de comenzar la transmisión, se establece el camino o ruta a seguir con una petición de llamada. Cuando la estación destino da el OK entonces se envía la información, y cuando este ha llegado, envía un aviso en el que se da a conocer que el paquete ha llegado y la red vuelve a estar disponible. Los paquetes tienen un identificador de circuito virtual en el destino y se reciben en el mismo orden que se enviaron.

Esta técnica otra ventaja que tiene es que en caso de que alguna trama contuviese un solo BIT erróneo, por defecto se volverá a enviar esa misma trama, solo el paquete afectado, en vez de todo el mensaje.

3.1.3 REDES DE CONMUTACIÓN DE MENSAJES

Esta técnica se usa principalmente para transmitir bits en redes digitales. Los nodos de conmutación son ordenadores con almacenamiento y reenvío a los que se les envía la

información del mensaje y la dirección del receptor, se van pasando la información de unos a otros hasta llegar al nodo final que estará comunicado con el receptor, la velocidad de esta transmisión es la máxima velocidad del enlace.

3.2 SEGÚN LA EXTENSIÓN

Cuando hablamos de las redes según su extensión, nos referimos a la distancia que son capaces de cubrir, según esta clasificación podemos encontrar tres tipos de redes. LAN, WAN, y MAN.

Las LAN son de las redes más conocidas, sus siglas significan Local Area Networks. Estas redes cubren distancias cortas, no más allá de diez kilómetros, y principalmente son redes de difusión y de velocidad alta. Suele estar entre 10 Mbps en Ethernet y los 100 Mbps en Fast Ethernet.

Ejemplos de LAN's son por ejemplo: 802.3 (Ethernet), 802.4 (Token Bus), 802.5 (Token Ring). Puede adquirir diversas tipologías como anillo, estrella, árbol, bus entre otras. Y la asignación del canal puede ser estática, por ejemplo Round Robind. O dinámica centrada o distribuida.

Por otra parte las redes WAN sus siglas significan Wide Area Networks, son redes de punto a punto y se usan para extensiones o distancias muy grandes, podemos hablar de más de cientos o miles de de kilómetros. Las máquinas están unidas por routers que hacen de almacenamiento y reenvío en el encaminamiento y sus topologías pueden ser muy variadas.

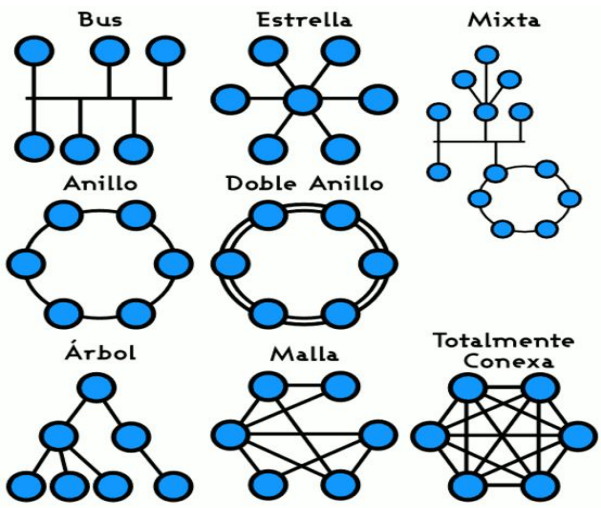
Finalmente queda por comentar las redes MAN, cuyas sigas significan Metropolitan Area Network. Al igual que las anteriores son redes de difusión y extensión media. Usan una tecnología muy similar a las LAN's, en éstas además no hay conmutación. Un ejemplo de este tipo de res son la 802.6 (DQDB).

4. TOPOLOGÍAS DE RED

Como hemos mencionado anteriormente las máquinas presentan distintos esquemas según se agrupen dando con ello lugar al término de "topología de red". Atendiendo a la topología podemos hacer una distinción entre física y lógica. La topología física, es como se dispone la red físicamente, pudiéndose referir también a como esté cableado.

La topología lógica es la forma que usa la red para reconocer a cada conexión de los distintos nodos.

Existen muchas topologías, algunas de las más conocidas son Bus, Anillo, Estrella o Malla, aunque a parte de éstas existan otras.



http://es.wikipedia.org/wiki/Archivo:Topolog%C3%Ada_de_red.png

4.1 TOPOLOGÍA BUS

La topología de BUS, consiste en un cable al cual se conectan todas las estaciones de trabajo. La información se manda de nodo a nodo sin que se puedan mandar información dos nodos a la vez, lo cual provoca colisiones. Cuando el emisor envía una información, ésta es escuchada por todas las máquinas, pero solo el receptor podrá usar los datos. Estas topologías son indicadas para sitios pequeños en lo que va a haber pocas máquinas. No se puede decir que sea muy eficiente puesto que solo un nodo puede enviar información a la vez, además si el

cable se daña entonces toda la red queda inutilizada por lo que hace de esta topología que sea un poco crítica en ciertos aspectos.

4.2 TOPOLOGÍA ESTRELLA

La topología de estrella consiste en que casa estación que se integra se dispone de tal manera que está conectada directamente al conmutador o hub que tenga la red. La ventaja de esta topología es que vamos a ganar en rapidez puesto que nos vamos a comunicar directamente con el conmutador y por lo tanto también vamos a evitar que se produzcan colisiones. Además de esto si una estación se cae no afecta al resto pudiendo seguir usando la red sin problema alguno.

4.3. TOPOLOGÍA ANILLO

Cada estación que se integra a la red lo hace de tal manera que forma un círculo, es decir, que está conectada a otras dos estaciones. Los conmutadores pueden estar en cualquier lugar del círculo, y la información se pasa entre las estaciones en el mismo sentido hasta que llega al destino. En este caso tampoco se pueden dar colisiones puesto que en la información van cabeceras con el destinatario y lo identifican de antemano.

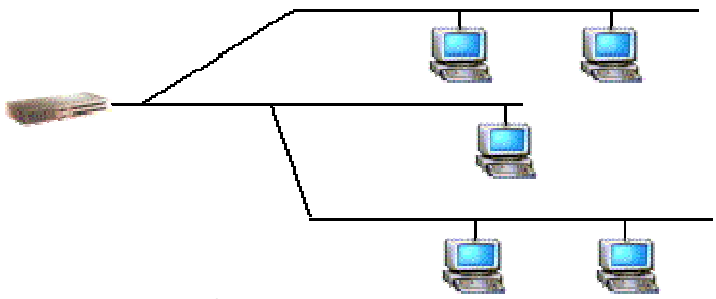
En este tipo de redes una desventaja que hay es que si se cae una estación se altera el comportamiento de toda la red. Además resulta una topología bastante cara de implantar.

4.4 TOPOLOGÍA MALLA

En ésta es tan fácil de explicar, como comentar que lo que hace es unir todas las estaciones entre sí, es decir, están conectadas todas con todas.

4.5 TOPOLOGÍA ÁRBOL

Esta topología al final viene a ser una ampliación de la topología de BUS, ésta cuenta con una raíz que sería el conmutador, y de este salen varias ramas que en el fondo son a su vez redes conectadas en BUS, como se puede apreciar en el dibujo.



http://web.frm.utn.edu.ar/comunicaciones/redes.html

5. PROTOCOLOS

Los protocolos los podemos definir como el lenguaje con el que se comunican dos máquinas, es necesario definir que comunican, como comunicarse y cuando lo comunican.

Con los protocolos podemos definir todas estas cosas. Según la información de *http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1* podemos ver la siguiente clasificación:

Los protocolos se pueden clasificar según su topología de red, pudiendo ser directos, si no hay máquinas intermedias, o indirectos como en redes de conmutación que es necesario algún agente intermedio.

Si la clasificación la hacemos según el tipo de terminal, podemos hablar de protocolos simétricos, si ambos extremos son iguales, o asimétricos si los comportamientos en cada extremo son distintos como en las de tipo cliente-servidor.

Según la forma de afrontar el problema podemos hablar de protocolos monolíticos si se

pretende resolver el problema de comunicación a la vez o de de protocolos estructurados si el problema se divide en partes de tal manera que cada parte la realice un protocolo.

Y finalmente también podemos clasificarlos según su normalización, pudiendo ser normalizados o no normalizados. Los primeros, son los definidos por las empresas de normalización para poder ser usados como estándares futuros. Y los segundos son diseñados para un problema de comunicación o tipo de red específicos, todos los protocolos originarios son no normalizados.

Algunos de los protocolos más conocidos y más usados son:

- IP (*Internet Protocol*)
- UDP (*User Datagram Protocol*)
- TCP (*Transmission Control Protocol*)
- DHCP (*Dynamic Host Configuration Protocol*)
- HTTP (*Hypertext Transfer Protocol*)
- FTP (*File Transfer Protocol*)
- Telnet (*Telnet Remote Protocol*)
- SSH (*Secure Shell Remote Protocol*)
- POP3 (*Post Office Protocol 3*)
- SMTP (*Simple Mail Transfer Protocol*)
- IMAP (*Internet Message Access Protocol*)
- SOAP (*Simple Object Access Protocol*)
- PPP (*Point-to-Point Protocol*)
- STP (*Spanning Tree Protocol*)
- SUPER (*Supreme Perpetued Resudict*)

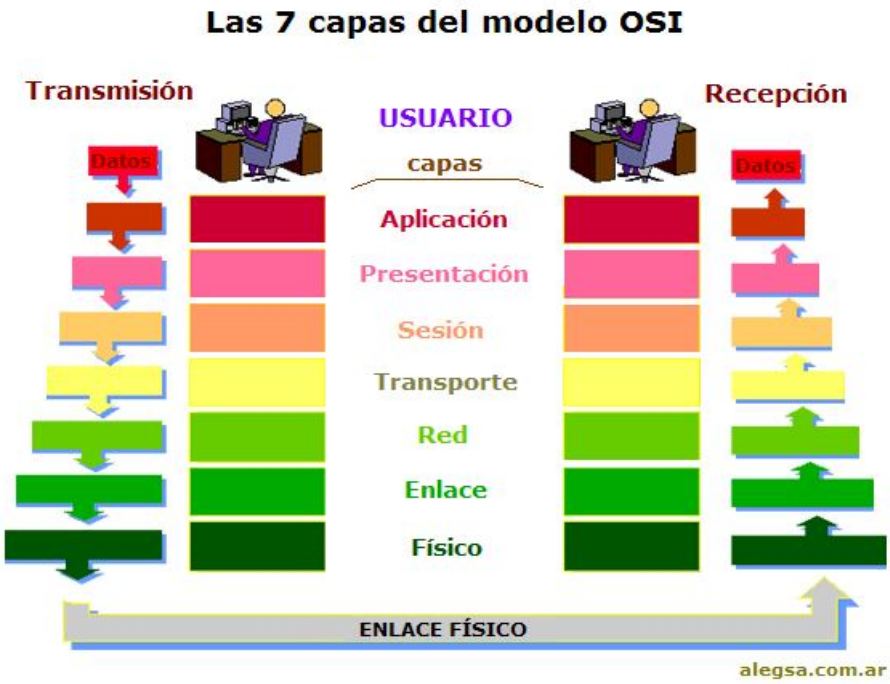
http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29

5.1 MODELOS DE REFERENCIA

5.1.1 MODELO OSI

Los modelos de referencia que tenemos hoy día son el modelo OSI origen de todo y el modelo TCP/IP.

Empezaremos con el modelo OSI por ser la referencia de los modelos actuales y por tanto ser también el más antiguo.



Como podemos comprobar en el dibujo, este modelo consta de siete capas:

CAPA1 Físico

CAPA 2 Enlace

CAPA 3 Red

CAPA 4 Transporte

CAPA 5 Sesion

CAPA 6 Presentación

CAPA7 Aplicación

5.1.2 NIVELES DEL MODELO OSI

5.1.2.1 CAPA FÍSICA

El nivel mas bajo es físico, en este nivel solo podemos hablar de ceros y unos que se transmiten a través del medio. La información sale de la máquina a la red. Este paso de información se hace a través de medios guiados como son todos los cableados, como UTP o fibra óptica, o medios no guiados como son los infrarojos, y las conexiones WiFi o inalámbricas. En este nivel podemos definir las caracteristicas del medio, electricas de la transmisión y funcionales del medio.En este nivel podemos hablar de la velocidad de trasmisión de los datos, y de la dirección de estos, que puede ser Simplex, si se transmite solo en una dirección, Duplex, si desde los dos nodos se puede enviar información y recibirla alternativamente, o Full Duplex si existen canales de envío y recepción simultaneos y en el cual no se dan colisiones.

5.1.2.2 CAPA DE ENLACE

Es la inmediatamente superior al nivel físico, en este nivel, su función principal es la detección de errores y el control del flujo. Envía a la capa superior la información correctamente. En las redes en las que entra en juego los conmutadores controla es establecimiento y liberación de la conexión además del buen funcionamiento de ésta.
También se encarga del control de acceso al medio compartido.

5.1.2.3 CAPA DE RED

Esta capa es la encargada de mantener la transmisión entre las máquinas a través de la propia red, se ocupa de toda la parte tecnológica de la comunicación y se usa para redes en las que haya conmutadores principalmente, asegura que la conexión sea fiable y llegue a su destino en este aspecto tecnológico.
El emisor tiene la dirección del receptor y es la propia capa de red la que se encarga de

encaminar toda la información por los canales.
Otras funcionalidades están muy bien descritas en el siguiente enlace:
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1

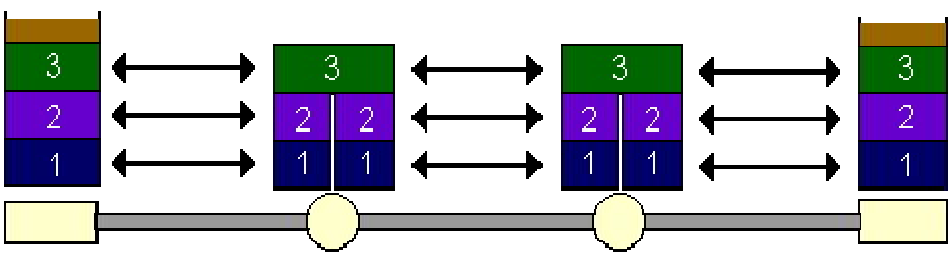
Cada nodo requiere un nivel físico y otro de enlace por cada medio de transmisión que le conecta a otro equipo. Sin embargo solamente requiere un nivel de red.

En redes de conmutación de circuitos, el nivel de enlace se encarga de mantener y liberar la conexión.

Si la red es de conmutación de paquetes por datagramas, entonces el nivel de red coge cada datagrama y decide por qué enlace enviar dicho datagrama.

Y si la red es de conmutación de paquetes por circuitos virtuales, es el nivel de red el encargado de establecer dicho circuito.

En caso de ser necesario el encaminamiento, la función corresponde al nivel de red.



5.1.2.4 CAPA DE TRANSPORTE

Esta capa acepta los datos que le van llegando de las capas superiores y los divide en partes más pequeñas si fuera necesario para después mandarlo al nivel de red. Todo este tratamiento de los datos lo hace independientemente del tipo de tecnología de rede que se esté usando. En este nivel hablamos de la información como segmentos. La función al final de cuenta es parecida a la del nivel de transporte pues en cierta manera controla que la información que llegue esté libre de errores, ordenado, sin duplicidades ni pérdidas. Al igual que en la capa anterior cabe destacar algunas características más que vienen bien descritas

en el mismo enlace:

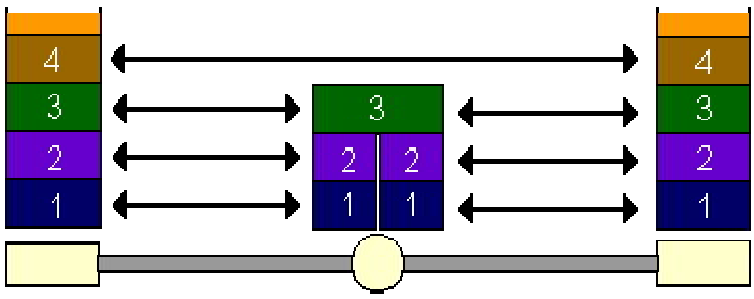
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1

En una red de conmutación de paquetes por datagramas, es el nivel de transporte el que se encarga de ordenar los distintos paquetes que llegan.

En las redes dedicadas y de difusión, no es necesario el nivel de transporte.

Este nivel es necesario exclusivamente en redes conmutadas o interconectadas. Requiere más trabajo en una red de conmutación de paquetes por datagramas que en una por circuitos virtuales, debido a la necesidad de ordenar los paquetes.

En las redes de conmutación de paquetes, este nivel se encarga de fragmentar el mensaje en el origen, y de recomponerlo en el destino.



5.1.2.5 CAPA DE SESIÓN

Como su propio nombre indica esta capa es la encargada de establecer la sesión entre dos máquinas. La sesión se establece principalmente para el intercambio de información y esta capa se ocupa de la sincronización de esos datos, del mensaje, la información, para que llegue en buen estado, para ello organiza grupos dentro del flujo de datos. También se encarga dentro de la conexión de establecer quién de los nodos tiene "el testigo" para saber cuándo enviar o recibir la información teniendo en cuenta que pueda darse una comunicación dúplex

o half-duplex. Esta capa también se ocupa de las conexiones a máquinas en remoto o intercambio de archivos entre éstas.

5.1.2.6 CAPA DE PRESENTACIÓN

En este nivel se eliminan los problemas consecuentes del intento de comunicar dos máquinas con distintas arquitecturas, puesto que dependiendo de cómo sea varía la forma de estructurar los datos. En este nivel la principal función es traducir las distintar arquitecturas que puedan darse en una misma comunicación para así establecer un lenguaje de datos común que entiendan las dos máquinas. En algunos casos también puede comprimir los datos y cifrarlos.

5.1.2.7 CAPA DE APLICACIÓN

Y finalmente hemos llegado a la última capa, la capa de aplicación, a este nivel ya podemos hablar de las aplicaciones a nivel de usuario. El proceso de datos ha terminado, y la comunicación ya ha quedado establecida y validada en todos los aspectos. Las aplicaciones tiran de este nivel.

5.1.3 PROTOCOLOS MÁS USADOS POR CADA NIVEL

- **Capa 1: Nivel físico**
  - Cable coaxial o UTP categoría 5, categoría 5e, categoría 6, categoría 6a Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.

- **Capa 2: Nivel de enlace de datos**
  - Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.

- **Capa 3: Nivel de red**
  - ARP, RARP, IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, Appletalk.

- **Capa 4: Nivel de transporte**
  - TCP, UDP, SPX.

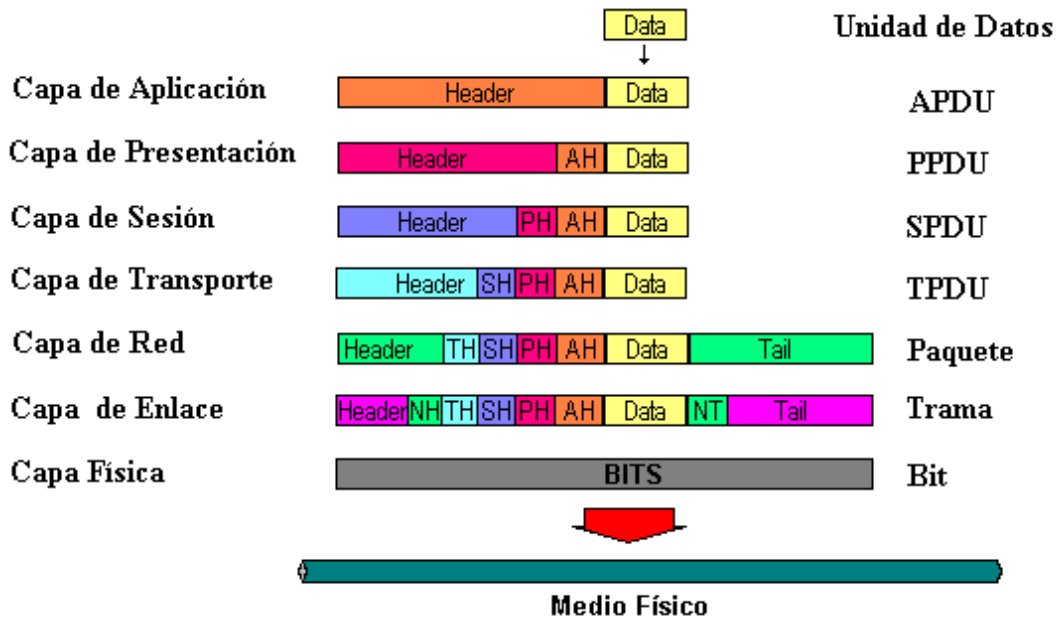
- **Capa 5: Nivel de sesión**
  - NetBIOS, RPC, SSL.

- **Capa 6: Nivel de presentación**
  - ASN.1.

- **Capa 7: Nivel de aplicación**
  - SNMP, SMTP, NNTP, FTP, SSH, HTTP, SMB/CIFS, NFS, Telnet, IRC, POP3, IMAP, LDAP.

http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29

5.1.3 ESTRUCTURA DE LOS DATOS POR NIVELES



APDU → Unidad de datos en la capa de aplicación *(Capa 7)*.

PPDU →Unidad de datos en la capa de presentación *(Capa 6)*.

SPDU →Unidad de datos en la capa de sesión *(Capa 5)*.

TPDU →(segmento) Unidad de datos en la capa de transporte *(Capa 4)*.

Paquete o Datagrama → Unidad de datos en el nivel de red *(Capa 3)*.

Trama → Unidad de datos en la capa de enlace *(Capa 2)*.

Bits →Unidad de datos en la capa física *(Capa 1)*.

http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29

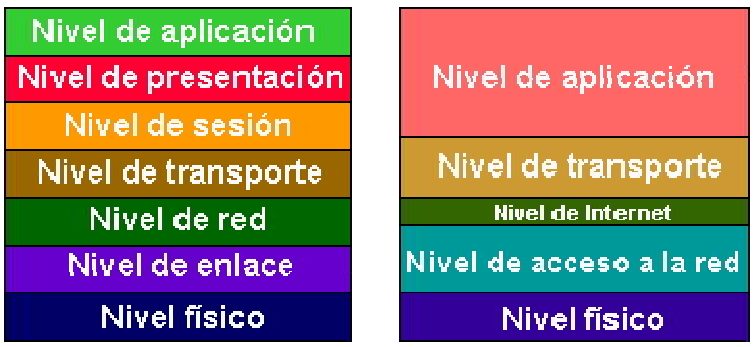
5.2 MODELO TCP/IP

Al igual en el modelo OSI, expresa cómo funciona la comunicación bajo las propias características de este modelo. Realmente el modelo TCP/IP está basado en el modelo OSI que fue el origen. Por lo tanto comparte muchas características con este primero y aporta nuevas formas de cómo establecer la comunicación que a continuación detallaremos.

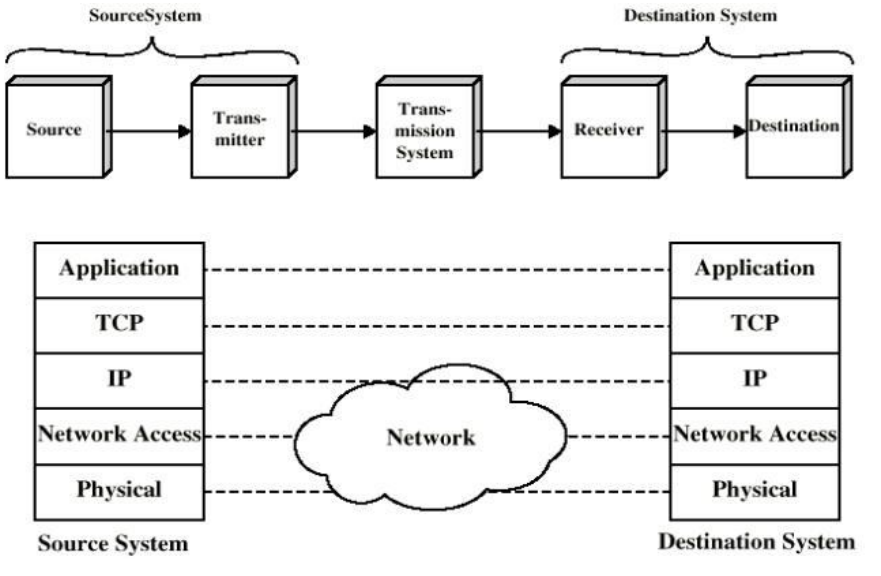
TCP/IP nace en 1972 en Estados Unidos y fue desarrollado por el departamento de defensa de dicho país siendo ejecutado por primera vez en ARPANET, que era una red de área extensa del departamento de defensa.

5.2.1 NIVELES DEL MODELO TCP/IP

En la siguiente imagen podemos apreciar el "acoplamiento" del modelo OSI en el modelo TCP/IP y las capas a las que queda reducido este modelo:



Al igual que en el caso anterior comprobamos que funciona similar:



http://trevinca.ei.uvigo.es/~mdiaz/rdo01_02/TEMA_5_archivos/image004.jpg

5.2.1.1 CAPA FÍSICA

En este caso, la capa física del modelo TCP/IP coincide exactamente con la capa física de OSI, por lo tanto, a este nivel se define el medio guiado o no, la naturaleza, velocidad de transmisión, codificaciones y demás.

5.2.1.2 CAPA DE ACCESO A RED

Se corresponde con el nivel de enlace y la mayor parte de del nivel de red del modelo OSI, por lo tanto agrupa en una sola capa ambos comportamientos. Es así que en este nivel se procede al intercambio de datos entre dos máquinas o sistemas electrónicos conectados a una misma red. Controla el interfaz entre un subsistema final y una subred por lo tanto especifica cómo deben enrutarse los datos utilicen la red que utilicen.

5.2.1.3 CAPA DE INTERNET

Se corresponde con el resto del nivel de red y es el encargado de conectar equipos que estén en redes diferentes. Usa el protocolo IP principalmente. Los datos atravesarán estas redes desde el emisor hasta el receptor.

5.2.1.4 CAPA DE TRANSPORTE

Incluye las capas de transporte y parte de la de sesión del modelo OSI. Se encarga de que la información llegue en el mismo orden en que fue enviada y sin errores, también puede usar algún mecanismo de seguridad, y los protocolos que usa mayormente son TCP orientado a conexión y seguro y UDP no orientado a conexión y no seguro.

5.2.1.5 CAPA DE APLICACIONES

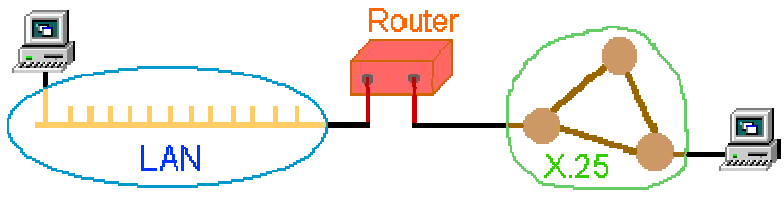
Este nivel se corresponde con las tres últimas capas del modelo OSI, es decir, parte de la capa de sesión, toda la de presentación y toda la de aplicación. En este nivel ya podemos hablar de que se ha producido la comunicación. Los protocolos más usados y conocidos son TELNET, FTP, HTTP, SMTP entre otros.

5.2.2 FUNCIONAMIENTO GLOBAL

Según el enlace:

http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1

Podríamos considerar que el funcionamiento global de este modelo consiste en que el router/encaminador se encargue de encaminar la información entre las distintas conexiones que haya, debido a las distintas redes. Los router IP unen redes tal como se puede ver:



Para que los equipos e puedan comunicar es necesario que lo hagan a través del protocolo IP que debe estar implementado en todos los casos, es decir, en todas las máquinas de las distintas redes que están interconectadas. Estas pequeñas redes dentro de una mayor se considera como una SUBRED y la unión de todas ellas forman Internet.

Para que la comunicación se pueda producir es necesario que las máquinas interconectadas posean una dirección IP del destinatario que será única.

También será necesario que haya una dirección del puerto al que corresponde la aplicación del destino que es la información a la que accedo en el receptor, esta dirección también es única pero en este caso, solo es única en el ordenador en concreto.

6. MEDIOS DE TRANSMISIÓN

Cuando hablamos de medios de transmisión estamos refiriéndonos al nivel físico, que a fin de cuentas es el encargado de enviar la información, de guiarla. Como se dijo anteriormente, estos medios de transmisión pueden ser guiados o no guiados. Las diferencias se detallan a continuación.

6.1 MEDIOS GUIADOS

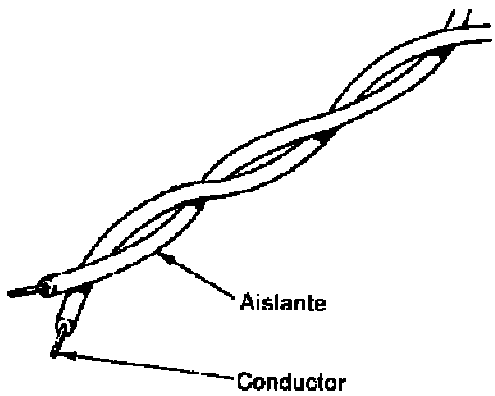
Cuando nos referimos a medios guiados podemos hablar de medios por los que se transmite la señal de la información. Un factor muy importante de la transmisión es la Velocidad o ancho de banda, que depende que la distancia entre la que se produzca la comunicación y del tipo de enlace como se explicó anteriormente pudiendo ser enlaces de punto a punto o de difusión.

El ejemplo más claro son los distintos tipos de cable, por poner un ejemplo, en cualquier CPD (Centro de Proceso de Datos), vemos muchos servidores conectados a los switches a través de fibra óptica, un acceso más rápido. Si estamos en casa o en una pequeña oficina, para conectar los equipos a las rosetas usaremos cables UTP.

A continuación haremos un mayor hincapié en los tres tipos de cables más conocidos y que por tanto son los que más se usan en una empresa.

6.1.1 PAR PRENZADO

Estos cables se componen de dos hilos conductores de cobre envueltos casa uno de ellos en un aislante y trenzados entre ambos para así evitar que se puedan separar. Al trenzar los cables lo que conseguiremos es que haya menos interferencias puesto que si se produce una de éstas afectaría a ambos cables de una manera lo más parecida posible.



http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

http://webs.um.es/barzana/II/Ii09_images/dgwzmf82_70dwgd36f3.jpg

6.1.1.2 TIPOS DE TRENZADO

6.1.1.2.1 UTP (*Unshielded Twisted Pair) (Par trenzado sin apantallar).*

Este tipo de cable es el más usado dentro del par trenzado, es sensible a interferencias entre los propios pares del cable como interferencias exteriores. La norma **EIA/TIA 568** empezó a dividir este tipo de cables según categorías. Actualmente estamos por la categoría 6.

- *Cat 1: actualmente no reconocido por TIA/EIA. Fue usado para comunicaciones telefónicas POTS, IGDN y cableado de timbrado.*
- *Cat 2: actualmente no reconocido por TIA/EIA. Fue frecuentemente usado para redes token ring (4 Mbit/s).*
- *Cat 3: actualmente definido en TIA/EIA-568-B. Fue (y sigue siendo) usado para redes ethernet (10 Mbit/s). Diseñado para transmisión a frecuencias de hasta 16 MHz.*
- *Cat 4: actualmente no reconocido por TIA/EIA. Frecuentemente usado en redes token ring (16 Mbit/s). Diseñado para transmisión a frecuencias de hasta 20 MHz.*
- *Cat 5: actualmente no reconocido por TIA/EIA. Frecuentemente usado en redes Ethernet, fast Ethernet (100 Mbit/s) y gigabit Ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz.*
- *Cat 5e: actualmente definido en TIA/EIA-568-B. Frecuentemente usado en redes Fast ethernet (100 Mbit/s) y gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz.*
    - *Nota sobre Cat 5e: Siendo compatible con Gigabit ethernet (1000 Mbit/s) se recomienda específicamente el uso de cable de Categoría 6 para instalaciones de este tipo, de esta manera se evitan perdidas de rendimiento a la vez que se incrementa la compatibilidad de toda la infraestructura.*
- *Cat 6: actualmente definido en TIA/EIA-568-B. Usado en redes gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 250 MHz.*
- *Cat 6a: actualmente definido en TIA/EIA-568-B. Usado en un futuro en redes 10 gigabit ethernet (10000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 500 MHz.*
- *Cat 7: actualmente no reconocido por TIA/EIA. Usado en un futuro en redes 10 gigabit ethernet (10000 Mbit/s). Diseñado para transmisión a frecuencias de hasta*

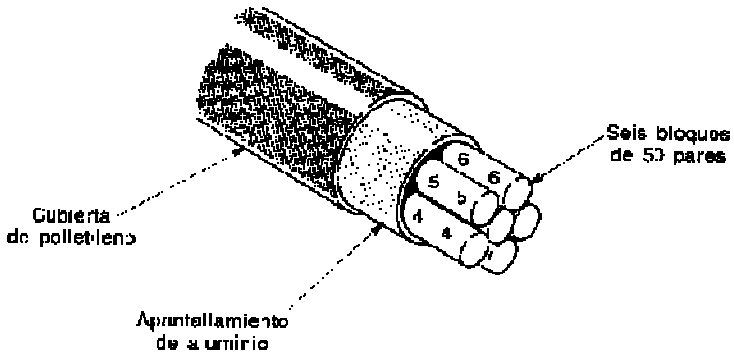
600 MHz.

http://es.wikipedia.org/wiki/Cableado_estructurado#Est.C3.A1ndares_de_Cables_UTP.2FSTP

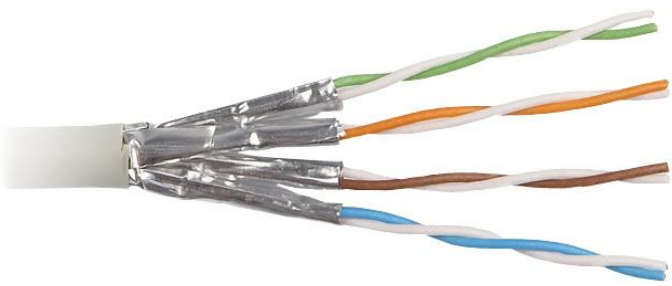
5.1.1.2.2 STP *(Shielded Twisted Pair)* (Par trenzado apantallado).

Contiene pares individuales envueltos por una malla metálica y a su vez todo el cable con todos los pares se envuelve también en otra malla para que se produzcan menos interferencias. Son cables más rígidos y más caros que los anteriores. Este modelo de cable está estandarizado por EIA/TIA 568 como un cable con impedancia de 50 Ω y frecuencia de 300 MHz. Siendo típicos los conectores RJ-45. Además gracias al apantallamiento podemos conseguir una mayor velocidad y ancho de banda.

Actualmente se vienen a usar en conexiones LAN y en la transmisión analógica y digital, (RDSI por ejemplo)



http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

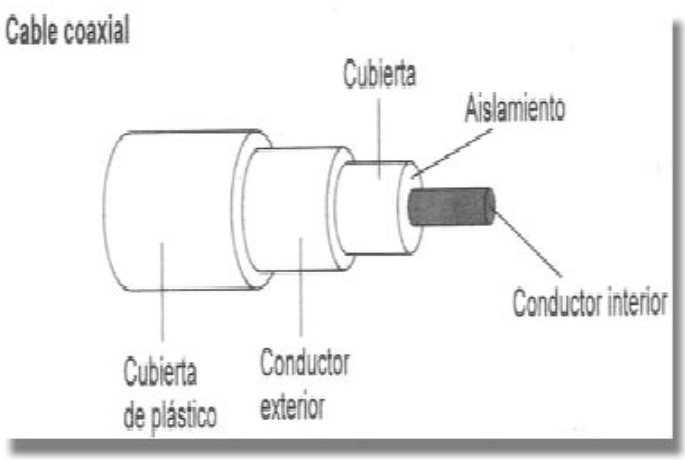


http://esp.hyperlinesystems.com/img/sharedimg/cable/stp4-c6-patch-ind.jpg

6.1.2 CABLE COAXIAL

Este cable consiste en dos conductores cilíndricos y concéntricos entre los que se coloca algún material dieléctrico, véase polietileno, PVC entre otros. Lleva una capa protectora que funciona como aislante. De este tipo de cable podemos comentar que ambos conductores del coaxial se mantienen concéntricos mediante unos discos y que la funcionalidad del conductor externo es hacer como una especie de pantalla que aísle en cierta medida las interferencias.

Este tipo de cable se usa especialmente en la transmisión de datos a mucha velocidad y distancias de kilómetros proporcionando por lo tanto un mayor ancho de banda entre todos los terminales conectados. Su frecuencia puede llegar a los 400 MHz.



http://docente.ucol.mx/al008353/public_html/imagenes/coaxial.jpg

http://radio.grupohg.es/tienda/images/RG11.jpg

Dentro de los cables coaxiales podemos distinguir tres tipos de estos, el coaxial estándar del tipo RG que se vienen utilizando para transmitir señales de televisión doméstica. Los cables con núcleos aislados por aire que se usan como retardadores en caso de incendios. Y finalmente los cables coaxiales de polietileno celular irradiado que son los más caros y apenas presentan diferencia con los anteriores.

6.1.3 FIBRA ÓPTICA

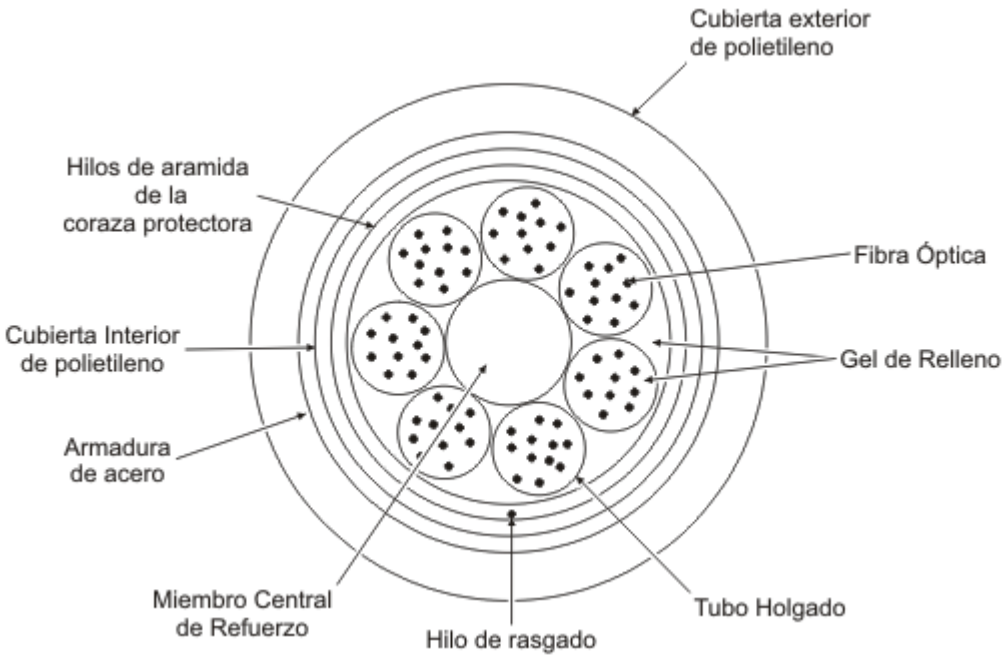
Estos cables están compuestos por un hilo muy fino de material transparente, vidrio o plástico por el cual se envían pulsos de luz.

La transmisión por este medio se basa en la diferencia del índice de refracción entre núcleo y cubierta la cual presenta un índice menor.

El núcleo transmite la luz y debido a cambios en el índice de refracción se da lugar a una reflexión total de la luz, de tal manera que muy poca luz sea la que se pierda en la fibra.

En función de ese cambio en el índice de refracción podemos distinguir fibras ópticas de índice a escala o monomodo y multimodo y fibras ópticas multimodo de índice gradual.

Pero en cualquier caso la principal cualidad de este tipo de medio en las redes de ordenadores es la velocidad. Mientras que los otros tipos de cables pueden llegar a alcanzar velocidades de hasta 100 Mbps como los cables UTP de categoría 5 que a día de hoy son los más usados, con la fibra óptica podemos alcanzar velocidades para usar en LAN’s de alta velocidad con Gigabit Ethernet.

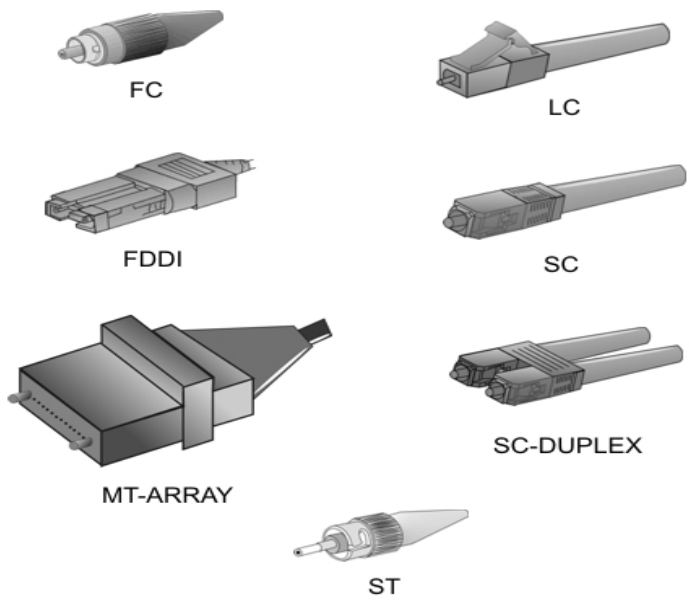


http://www.textoscientificos.com/imagenes/redes/fibraoptica-armadura.gif

http://informatica.temuco.udelmar.cl/~lmachuca/dokuwikilucho/_media/proyectos/taller-redes/contenidos/cable-fibra-optica.jpg

6.1.3.1 TIPOS DE CONECTORES

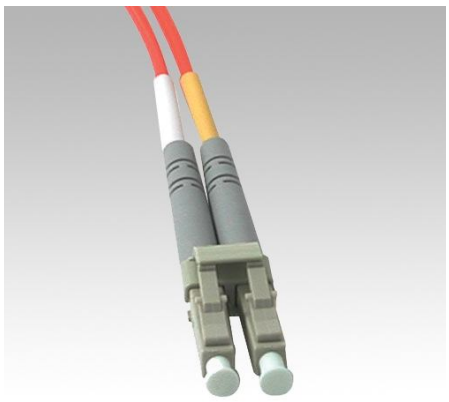
Los extremos de la fibra óptica no tienen por qué ser iguales. Como podemos apreciar en la imagen existen diversos tipos de terminales, los cuales en un mismo cable podemos combinar en los extremos:



http://grupos.emagister.com/imagen/tipos_conectores_fibra_optica/t269986-0.jpg

En esta imagen podemos ver fibras con distintos conectores.

http://www.timbercon.com/Cables-de-Fibra-Optica/Cables-de-Fibra-Optica.jpg



http://www.electronica-basica.com/images/cable-fibra-optica2.jpg

Todos estos conectores se pueden combinar en los extremos de un mismo cable.

CAPÍTULO III
INTRODUCCIÓN A LA AUDITORÍA

1. INTRODUCCIÓN A LA AUDITORÍA

Primeramente abarcaremos en términos globales lo que es y supone una auditoría para luego centrarnos en el tema esencial de este proyecto que es la auditoría de sistemas de información.
Podemos definir la auditoría cómo manera de examinar en profundidad un objeto sometido a análisis con el objetivo de determinar si existen anomalías o falta de fiabilidad ya sea de la información o falta de cumplimentación de las condiciones prescritas.
Algunos de los tipos de auditorías que podemos encontrar son: Auditorías de estados financieros, informes económicos, auditoría interna, operativa, de sistemas o económico social.

AUDITORÍA EN INFORMÁTICA

Centrándonos más en el concepto de la auditoría en informática podemos definirla como: (www.info-ab.uclm.es/asignaturas/42602/introauditoría.pdf)

Alcanzar una opinión sobre el sistema de información y sobre los datos que se procesan debiendo ser éstos exactos, completos y autorizados. Los errores deben ser detectados y corregidos a tiempo, y deberán existir procedimientos adecuados y actualizados que garanticen la continuidad de sus operaciones.

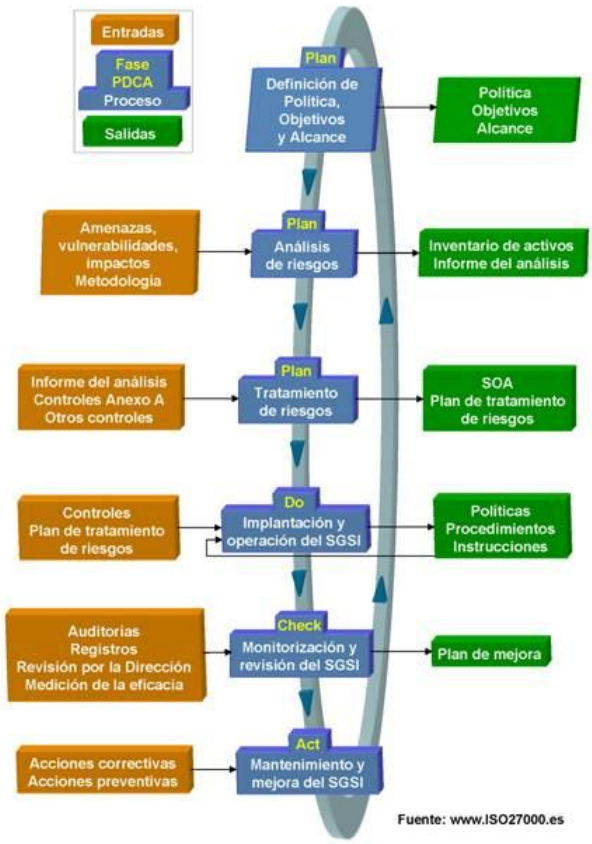
Los objetivos de la auditoría informática son entre otros:

- La verificación de aspectos organizativos y administrativos de la función de procesos de datos.
- Verificación de los controles del ciclo de vida de un sistema.
- Verificación de los controles de acceso a instalaciones, terminales, librerías, etc.
- Mecanización de las actividades de la auditoría interna.
- Colaboración con los auditores externos.

AUDITORÍA EN SISTEMAS DE INFORMACIÓN

Para llevar a cabo la auditoría necesitamos elaborar un plan en el que se definan los objetivos, el alcance, necesitamos que haya un conocimiento previo y análisis de los procedimientos del estándar a aplicar. Necesitamos llevar a cabo una evaluación de controles internos y procedimientos y pruebas.

Dentro de la auditoría en sistemas de información se sugiere llevar a cabo controles directivos, preventivos, de detección, correctivos, y de recuperación.
Los objetivos de control serán declaraciones sobre el resultado final deseado o a lo que se desea llegar mediante las protecciones y los procedimientos de control.
Las áreas que puede cubrir la auditoría en sistemas de información abarca desde controles directivos, medidas de desarrollo, verificación de si se ajusta a la legalidad, amenazas físicas externas, control de acceso adecuado, protección de datos, comunicaciones y redes que es nuestro tema central, áreas de producción, desarrollo de aplicaciones en entornos seguros y la continuidad de las operaciones.



Finalmente nombrar los principios del auditor informático:

- Principio de beneficio del auditado.
- Principio de calidad.
- Principio de capacidad.
- Principio de cautela.
- Principio de comportamiento profesional.
- Principio de concentración en el trabajo.
- Principio de confianza.
- Principio del criterio propio.
- Principio de discreción.
- Principio de economía.
- Principio de formación continuada.
- Principio de fortalecimiento y respeto a la profesión.
- Principio de independencia.
- Principio de información suficiente.
- Principio de integridad moral.
- Principio de legalidad.
- Principio de libre competencia.
- Principio de no discriminación.
- Principio de no injerencia.
- Principio de precisión.
- Principio de secreto profesional.
- Principio de veracidad.
- Principio de servicio público.

Buscando en:

http://www.isaca.org/Template.cfm?Section=Standards&CONTENTID=49806&TEMPLATE

IT Audit and Assurance Tools and Techniques

Issued by the Standards Board of ISACA®

Click on the document name to view it in HTML or click on the icon to view or download the document as a PDF.

IT Audit and Assurance Tools and Techniques		Effective Date
P1	**IS Risk Assessment Measurement**	**1 July 2002**
P2	**Digital Signatures**	**1 July 2002**
P3	**Intrusion Detection**	**1 Aug 2003**
P4	**Viruses and Other Malicious Code**	**1 Aug 2003**
P5	**Control Risk Self-assessment**	**1 Aug 2003**
P6	**Firewalls**	**1 Aug 2003**
P7	**Irregularities and Illegal Acts**	**1 Nov 2003**
P8	**Security Assessment—Penetration Testing and Vulnerability Analysis**	**1 Sept 2004**
P9	**Evaluation of Management Controls Over Encryption Technologies**	**1 Jan 2005**
P10	**Business Application Change Control**	**1 Oct 2006**
P11	**Electronic Funds Transfer (EFT)**	**1 May 2007**

=/ContentManagement/ContentDisplay.cfm

2. TEMAS A TRATAR

Así en general en estos enlaces tenemos acceso a distintos puntos que en cierta manera son todos ellos parte de las redes a evaluar. Los puntos más interesantes son:

- P2 Firma digital.
- P3 Detección de intrusos.
- P4 Código malicioso y virus.
- P6 Cortafuegos.
- P8 Evaluación de seguridad, pruebas, análisis de vulnerabilidad.

P2 FIRMA DIGITAL

En este punto primeramente se comenta que el objeto de este procedimiento es proporcionar un medio a la entidad certificadora en términos de calidad como de fiabilidad de los servicios ofrecidos.

A continuación el texto comenta la importancia que tienen estos métodos de cara al comercio electrónico, a servicios como una intranet o transacciones ya sean personales o comerciales, es evidente que es de gran importancia puesto que en caso contrario sería un agujero de seguridad por el cual se podría tener acceso a datos protegidos y con lo que se podría hacer un uso indebido con todo lo que ello conlleva, ya sea de cara a un utilitario o de una organización.

Prosigue tratando el tema en que la autenticación se puede realizar desde distintos niveles de seguridad y por distintas tecnologías. Comenta cómo antes se utilizaban unas contraseñas muy similares entre servidores por ejemplo o contraseñas de muy baja protección. Esto ha pasado y sigue pasando en la actualidad aunque sí es verdad que ya cada vez en menor medida. Casos como por ejemplo tener un usuario: Pepito y una contraseña: Pepito. Además cada vez se hace más hincapié en el tema de usar para las contraseñas mayúsculas combinadas de minúsculas y números, y por lo general tener una longitud que ronde los ocho

dígitos. Esto de cara a un hacker le hace más difícil la tarea de poder encontrar las contraseñas de accesos ya sean al medio que sean. En cualquier caso para asegurarnos una correcta protección de los datos lo más seguro es usar los método de autenticación de clave pública o algunos de los métodos que se están extendiendo ahora como el uso de sistemas biométricos o uso de claves criptográficas para la autenticación.

P3 DETECCIÓN DE INTRUSOS

Otro de los puntos que comentamos anteriormente es el P3 que trata sobre la detección de intrusos.

En este punto primeramente se trata los antecedentes, comenta la transmisión de las normas. Nombra la norma S6 como el desempeño de los sistemas de trabajo de la auditoría y expone literalmente:

"Durante el curso de la auditoría, el auditor deberá obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de la auditoría. Los resultados de la auditoría y las conclusiones han de basarse en un análisis adecuado y la interpretación de esta evidencia. "

A continuación relaciona la detección de intrusos con Cobit:

"Es responsabilidad de la administración para salvaguardar todos los activos de la empresa. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la gerencia debe establecer un sistema adecuado de control interno."

El punto siguiente comenta que las directrices para la gestión Cobit, proporcionan un marco de gestión orientado para el control continuo y proactivo de la auto-evaluación. En general todos estos puntos siguientes comentan temas de negocio relacionados con el mismo Cobit, pero realmente al no estar especialmente relacionados con el tema bastaría sólo con lo arriba expuesto.

Llegados al punto 1.3 se explica algo más interesante en relación al tema, se exponen los procedimientos a llevar a cabo los auditores para detectar una posible intromisión de intrusos. Desde ahora las referencias a Sistemas de Detección de Intrusos lo denotaremos como IDS.

Los temas a tratar serán:

- Definición de un IDS y cómo funciona.
- El propósito y los beneficios de la utilización de un IDS.
- Los principales tipos de IDS y las ventajas y desventajas de cada orientación sobre las condiciones necesarias para aplicar y administrar adecuadamente un IDS.
- Planificación de las consideraciones en la revisión de un IDS.
- Una visión general del enfoque de auditoría.
- Informes y cuestiones.
- Tipos de procedimientos de auditoría y pruebas de auditoría.

La numeración que aparece a continuación se corresponde con la de la documentación original.

2.

¿QUÉ ES UN IDS?

2.1 Definición

2.1.1 La detección de intrusiones es el proceso de detectar el uso no autorizado de sistemas y redes a través del uso de software especializado y / o hardware. El propósito principal de un IDS es ofrecer la posibilidad de ver la red y la actividad del sistema en tiempo real y para identificar la actividad no autorizada. Además, puede proporcionar una respuesta automática casi en tiempo real. Los productos IDS también ofrecen la posibilidad de analizar la actividad de hoy en relación con la actividad el pasado para identificar las tendencias y los problemas más grandes.

2.2 Objetivos y beneficios de un IDS

2.2.1 El propósito principal de realizar la detección de intrusos es ayudar a prevenir las consecuencias causadas por intrusiones sin ser detectados. La implementación de un programa de controles de seguridad efectiva es un buen punto de partida para establecer la infraestructura de seguridad de apoyo. Los controles eficaces surgen de políticas eficaces de seguridad de la información, estándares y prácticas y el uso de tecnología apropiada. La tecnología apropiada se define como la tecnología que apoya y aplica las políticas de una organización eficaz. Ser capaz de detectar un intento de intrusión en tiempo real es un aspecto importante de la detección de intrusiones. Saber cuándo un ataque está en curso y ser capaz de tomar una acción inmediata mejora significativamente las probabilidades de éxito. La detección en tiempo real depende de contar con un sistema de vigilancia que se encuentra en segundo plano y supervisa todas las actividades relacionadas con los dispositivos conectados. El sistema de monitoreo debe ser capaz de interpretar varios incidentes y diagnosticar los ataques reales.

2.2.2 La mayoría de los IDS tradicionales suelen consistir en tomar una red o tomar un enfoque basado en host hacia la identificación y la protección contra ataques. Éstos buscan firmas de ataques, las pautas específicas que normalmente indican la intención maliciosa o actividad sospechosa. Un método verdaderamente eficaz de IDS es emplear ambos métodos.

2.3 Tipos principales de IDS

2.3.1 Los principales tipos de IDS son:

- *Basado en host*
- *Basados en la red*
    - *- Estadística anomalía*
    - *- Coincidencia de patrones*

2.4 IDS basados en host

2.4.1 La detección de intrusos basado en host se inició en la década de 1980 antes del uso de redes tan frecuentes, complejas e interconectadas como en la actualidad. En este entorno más sencillo, era común la práctica de revisar los registros de auditoría para detectar actividades sospechosas. Debido a que las intrusiones fueran raras, después de los análisis ha resultado ser suficiente para prevenir futuros ataques.

2.4.2 Los IDS basado en host todavía utilizan los registros de auditoría, pero son mucho más automatizado, habiendo evolucionado para incluir técnicas de detección más sofisticadas y sensibles. IDS basado en host normalmente controlan los sistemas, eventos y registros de seguridad. Cuando alguno de estos archivos cambio, el IDS se compara con el registro de nuevas firmas de ataques para determinar si hay alguna coincidencia. Si es así, el sistema responde con las descripciones de administrador y otras llamadas a la acción. Efectuará un seguimiento de archivos en sistemas de cambios. El objetivo principal IDS basado en host es monitorear los sistemas de cambios en los archivos individuales.

2.4.3. Los IDS basado en host se ha ampliado para incluir otras tecnologías. Un método popular es detectar intrusiones sobre archivos clave del sistema y ejecutables a través de sumas de ciclo de redundancia cíclica o CRC que buscan cambios inesperados. La puntualidad de la respuesta está directamente relacionada con la frecuencia del intervalo de sondeo.

2.4.4 Los IDS basados en host no son tan rápidos como sus homólogos basados en red, sin embargo, sí ofrecen ventajas que los sistemas basados en la red no pueden igualar. Estas ventajas incluyen mayor análisis, mejor enfoque acerca de datos de eventos específicos del sistema y reducir los costos de nivel de entrada.

2.4.5 Las ventajas de IDS basados en host incluyen:

Que se verifique el éxito o el fracaso de un ataque. Mientras IDS basado en red proporcionan una alerta temprana, IDS basados en host puede prever si un ataque fue exitoso o no. Pueden llevar un seguimiento de las actividades específicas del sistema.

Los IDS basados en host pueden supervisar toda la actividad del usuario mientras está conectado a la red. Es muy difícil para un sistema basado en red proporcionar este nivel de detalle del evento. También detectan ataques que no son identificados por los sistemas basados en red. Están bien adaptados para cifrado y cambio de entornos. Dado que los sistemas basados en host residen en máquinas distintas a través de una empresa, pueden superar algunos de los problemas de los sistemas basados en la red de conmutación de entornos y cifrado. Identificar dónde colocar el IDS específicamente en las redes internas puede ser difícil cuando se trata de ofrecer una amplia cobertura para la empresa. En un sistema basado en host, el flujo de datos ya ha sido descifrado. Se han multiplicado prácticamente en tiempo real la detección y respuesta. Muchos sistemas actuales basados en host pueden recibir una interrupción del sistema operativo cuando hay una entrada de registro de archivo nuevo. Esta nueva entrada puede ser procesada de inmediato, reduciendo significativamente el tiempo entre el reconocimiento de ataques y la respuesta. Ellos no requieren hardware adicional. Los IDS basado en host residen en la infraestructura de red existente, incluyendo servidores de archivos, servidores Web y otros recursos compartidos. Ellos tienen un menor coste de entrada. Los IDS basados en red pueden ofrecer una amplia cobertura con poco esfuerzo y con frecuencia son caros. Las intrusiones basadas en host de detección son a menudo un precio muy alto por un solo agente y pueden ser desplegados con una financiación inicial limitada.

2.4.6 Las desventajas de los IDS basados en host:

Sus capacidades se ven comprometidas en cuanto el equipo host se vea comprometido. Añaden sobrecarga adicional a un sistema operativo y requieren una copia para cada máquina en una red protegida. Con frecuencia se compara con las herramientas de antivirus, para que los usuarios tiendan a utilizar sólo el antivirus, cuando el IDS proporciona características de seguridad que no se encuentran en un software de antivirus.

Son muy específicas de la aplicación. Deben ser capaces de traducir entre Windows, UNIX y otros sistemas. Como parte de estos sistemas reside en el host que está siendo atacado, los IDS basados en host pueden ser atacados por un atacante inteligente.

No son adecuados para la detección de escaneos de red de todos los hosts en una red. Desde el IDS en cada host sólo se ven los paquetes de red que específicamente recibe. A menudo tienen dificultades para detectar y operar durante los ataques de denegación de servicio. Utilizan los recursos informáticos de los hosts que están monitoreando.

2.5 IDS basado en red

2.5.1 Los IDS basados en red pueden usar los paquetes de red como el origen de datos. Los IDS basados en red suelen utilizar los adaptadores de red funcionando en modo promiscuo para monitorear y analizar el tráfico de red en tiempo real. El modo promiscuo hace que sea extremadamente difícil detectar y localizar al atacante. Un ataque de reconocimiento utiliza dos técnicas comunes para reconocer una firma de ataque:

- *Estadística de las detecciones de anomalías*
- *Diseño, expresión o código de bytes.*

2.5.2 Las ventajas de IDS basados en red son:

Su mayor activo es el sigilo. Pueden ser desplegados sin efecto sobre los sistemas existentes o de infraestructura. La mayoría son independientes del sistema operativo. La implementación de sensores de detección de intrusos basados en red va a escuchar de todos los ataques, sin importar el tipo de sistema operativo de destino.

2.5.3 Las desventajas de los IDS basados en red son:

Primeramente que no son muy escalables, han luchado por mantener la capacidad de 100 Mbps. Se basan en firmas de ataques predefinidos. Los proveedores de IDS no han alcanzado todos los ataques conocidos, y las actualizaciones de firmas no son liberadas tan frecuentemente como las actualizaciones de antivirus.

2.6 IDS de anomalía estadística

2.6.1 En el modelo de detección de anomalías, el IDS detecta intrusiones en busca de una actividad que es diferente a la de un usuario o sistema. La anomalía IDS se ha basado en establecer las líneas básicas de la conducta normal de perfiles de usuarios o conexiones de red y, a continuación de seguimiento de las actividades que se apartan de la línea de base.

2.6.2 Las ventajas de IDS basado en estadísticas anomalía incluyen: Muchos expertos de seguridad creen que son capaces de detectar lo nunca antes visto en ataques, a diferencia de los IDS basado en el patrón de igualación que se basan en el análisis de ataque de la firma de los ataques del pasado. Pueden detectar un comportamiento inusual y por lo tanto tienen la capacidad de detectar ataques sin tener que ser programados específicamente para detectarlas.

2.6.3 Las desventajas de la estadística anomalía IDS basado incluyen: A menudo producen un gran número de falsos positivos debido a la naturaleza impredecible de los usuarios y redes. La detección de anomalías basado en enfoques conjuntos a menudo requieren una amplia capacitación de los registros de sucesos del sistema para caracterizar los patrones normales de comportamiento. Los hackers cuidadosamente pueden evadirlos o deshabilitarlos.

2.7 IDS de patrones

2.7.1 La mayoría de los productos comerciales se basan en el examen del tráfico en busca de patrones de ataque ya documentados. Esto significa que el IDS es programado para identificar una conocida técnica de ataque. Esto. El ejemplo clásico es el de examinar todos los paquetes en el segmento de red para un patrón definido de la actividad que indica un intento de acceder a un script vulnerables en un servidor Web. Algunos IDS se construyen a partir de grandes bases de datos que contienen miles de tales patrones. El IDS supervisa todos los paquetes, en busca de los paquetes

que contienen uno de estos patrones definidos.

2.7.2 Las ventajas de la coincidencia de patrones IDS incluyen:

Un calendario de aplicación más cortos que los IDS anomalía. Sin embargo, debe haber un motor de reconocimiento de patrones que se ejecutan en la red que busca eventos que se ajustan a las definiciones patrón específico.

Son fáciles de implementar, desplegar, actualizar y comprender. Producen menos falsos positivos, en comparación con anomalía de IDS ya que producen un mayor número de falsos negativos. En otras palabras, es más fácil caer algo más allá de un patrón de coincidencia sistema de detección, pero son rápidos.

2.7.3 Las desventajas de un patrón de coincidencia IDS incluyen:

El tráfico normal de red provoca muchos falsos positivos, pero menos en relación con las anomalías de los IDS basados en estos patrones. Los hackers cuidadosamente pueden evadir o deshabilitar el IDS. Ellos no pueden detectar cualquier cosa por que no tienen un patrón. Requieren de una actualización constante con las nuevas normas. Son más fáciles, en comparación con los IDS basados en anomalías, para engañar mediante el envío de paquetes fragmentados a través de la red.
La mayoría de las actualizaciones de patrones son proporcionadas por el proveedor del IDS, dando un papel en la seguridad de la red al vendedor. La capacidad del proveedor para ofrecer las pautas para los ataques recién descubiertos es una clave en el mantenimiento de una efectiva utilización de IDS de patrones.

P4 CÓDIGO MALICIOSO Y VIRUS

El punto expuesto a continuación es el P4 que trata sobre virus y código malicioso. Primeramente se enfoca el documento desde la perspectiva de que debe existir un documento en el que quede reflejado las políticas de seguridad que son llevadas a cabo por parte de la empresa para la detección y corrección de estos códigos maliciosos y virus.

En relación con COBIT expone lo siguiente:

1. Relación con el COBIT

1.2.1 Los estados COBIT. Marco: "Es responsabilidad de la administración para salvaguardar todos los activos de la empresa. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la gerencia debe establecer un sistema adecuado de control interno."

1.2.2 Las Directrices para la Gestión COBIT proporcionan un marco de gestión orientado para el control continuo y proactivo de auto-evaluación se centró específicamente en:

Medición del desempeño-¿La función de TI apoya los requerimientos del negocio? Perfiles de control de TI-¿Qué procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control? Concienciación -¿Cuáles son los riesgos de no alcanzar los objetivos? Benchmarking-¿Qué hacen otros? ¿Cómo pueden los resultados medir y comparar?

1.2.3 Las Directrices de administración proporcionan métricas ejemplo que permite la evaluación de desempeño de TI en términos de negocio. Los principales indicadores para identificar y medir los resultados de las TI, y los indicadores clave de rendimiento evaluar la eficacia de los procesos que se realizan mediante la medición de los facilitadores del proceso. La madurez de los modelos y de los atributos proporciona evaluaciones de capacidad y la evaluación comparativa, ayudar a la administración para medir la capacidad de control y determinar las deficiencias de control y estrategias de mejora.

1.2.4 Las Directrices de Gestión se pueden utilizar para apoyar talleres de autoevaluación, y también se puede utilizar para apoyar la aplicación por la gestión de la vigilancia continua y procedimientos de mejora como parte de una estructura de gobierno de TI.

1.2.5 COBIT ofrece un conjunto detallado de controles y técnicas de control para el entorno de la información de administración de sistemas. La selección del material más relevante en COBIT aplicable al ámbito de la auditoría especial se basa en la elección de COBIT en procesos de TI y la consideración de los criterios de

información de COBIT.

El siguiente punto ya entra más en el tema central de los virus y código malicioso o *malware*. En estos casos el auditor es el encargado de proporcionar garantía a la empresa de la organización cuenta con los procedimientos adecuados sobre prevención, detección y corrección de los virus. Todo esto además deberá estar correctamente documentado. La idea de esto es que el auditor aplique los controles sobre lo anteriormente expuesto a través de la documentación que la propia organización le proporciona para ver si es consistente y suficiente en caso de ser necesario aplicarla.

El punto 3 son las tablas con técnicas para evaluar la eficacia de las políticas ante casos de virus, o códigos maliciosos.

Y el punto 4 trata sobre la presentación de informes. Explica que los usuarios son los responsables de sus propios equipos y que en caso de tener duda acerca de si sus equipos pudieran estar infectados es su deber parar de usar las máquinas y proceder a mandar una incidencia a las partes apropiadas, ya sean departamento de seguridad, *help-desk*, o lo que sea relevante, para poder levar a cabo los procedimientos de limpieza de equipo en caso de ser necesario para evitar la propagación de los virus en la empresa.

P6 CORTAFUEGOS

Seguimos con el punto P6: Cortafuegos.

El tema a tratar es una parte esencial en el tema de la seguridad de tal manera que estos están para hacer las filtraciones necesarias para evitar accesos no autorizados al sistema.

Comenzando por el punto primero se comenta sobre el tema de auditorías lo descrito por regla general de que el personal auditor es el encargado de comprobar que se cumplen las normas y los objetivos de la empresa en el campo que se abarque.

Al igual que en puntos anteriores se explica la relación de este tema de cortafuegos con Cobit describiendo lo siguiente:

1. Relación con el COBIT

1.2.1 Los estados COBIT: "Es responsabilidad de la administración salvaguardar todos los activos de la empresa. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la gerencia debe establecer un sistema adecuado de control interno."

1.2.2 Las Directrices para la Gestión COBIT proporcionan un marco de gestión orientado para el control continuo y proactivo de auto-evaluación centrado específicamente en:

Medición del desempeño- ¿Qué tal es la función de TI para apoyar los requerimientos del negocio? Perfiles de control de TI- ¿Qué procesos de TI son importantes? ¿Cuáles son los factores críticos de control para el éxito? Concienciación-¿Cuáles son los riesgos de no alcanzar los objetivos? Benchmarking- ¿Qué hacen otros? ¿Cómo pueden los resultados medir y comparar?

1.2.3 Las Directrices de administración proporcionan métricas ejemplo que permiten la evaluación y desempeño de TI en términos de negocio. Los principales indicadores de identificar y medir los resultados de los procesos de TI, y los indicadores clave de rendimiento para evaluar la eficacia de los procesos, se realizan mediante la medición de los indicadores del proceso. La madurez de los modelos y los atributos proporcionan evaluaciones de capacidad y la evaluación comparativa, ayudar a la administración para medir la capacidad de control y determinar las deficiencias de control y estrategias de mejora.

1.2.4 Las Directrices de Gestión se pueden utilizar para apoyar talleres de autoevaluación, y también se puede utilizar para apoyar la aplicación por la gestión de la vigilancia continua y procedimientos de mejora como parte de una estructura de gobierno de TI.

1.2.5 COBIT ofrece un conjunto detallado de controles y técnicas de control para el entorno de la información de administración de sistemas. Selección del material más relevante en COBIT aplicable al ámbito de la auditoría especial se basa en la elección

de procesos específicos de COBIT de TI y la consideración de criterios de información de COBIT.

El punto 1.3 explica un poco como ha sido la evolución en este aspecto.

EVOLUCIÓN

1.3.2 Las empresas modernas se organizan como un conjunto de procesos básicos que operan en redes de suministro y la demandan. Casi todas las organizaciones en el mundo se enfrentan a una creciente presión para la eficacia y la eficiencia (es decir, mayores requisitos de calidad para los productos y servicios, el aumento de los ingresos, reducción de costos, desarrollo de nuevos productos), una presión para mejorar los procesos más rápidos y más baratos. Estas redes cada vez más complejas operan y se apoyan en tecnologías de comunicación disponibles (sobre todo Internet), permitiendo a las empresas centrarse en sus competencias básicas y asociarse con otros para ofrecer un valor agregado a los clientes.

1.3.3 La transformación de los antiguos procesos está habilitado de nuevos canales de comunicación. Estos canales ofrecen nuevas posibilidades de vinculación entre los diferentes sistemas y redes, poniéndolas a disposición de más personas dejando las entidades y sus procesos de interacción, como por ejemplo, *e-procurement* y *e-sourcing*.

1.3.4 Estos nuevos procesos han mostrado la necesidad de nuevas técnicas para permitir el acceso autorizado a los datos de una organización y los programas y protegerlos de los no autorizados (y sobre todo maliciosos) el acceso a través de los nuevos canales que interconectan las redes existentes con fuentes externas. En vista de ello, el equipo ha desarrollado tipos especiales de funcionalidad (*firewalls*) que ayudan a minimizar los riesgos mencionados anteriormente.

1.3.5 Existen varios tipos de servidores de seguridad y se utilizan en varias configuraciones diferentes, cada una adecuada para una necesidad de protección específica.

1.3.6 Este documento ofrece orientación para auditores que cada vez se encuentran

con que tienen auditoría o revisión de nuevos procesos que interconectan las distintas entidades a través de medios como Internet, las conexiones directas y las redes arrendadas, y por lo tanto tienen que evaluar la fuerza de las barreras de protección para ofrecer garantías razonables de la integridad de la información, confidencialidad y disponibilidad.

El punto 2 ya entra más en concreto con los

CORTAFUEGOS

Un *firewall* está diseñado como una parte del sistema o de la red para bloquear accesos no autorizados. Con éstos se puede cifrar el tráfico de red según las normas establecidas.

Algunos de los tipo de cortafuegos que existen son los de nivel de aplicación de pasarela que son los más habituales siendo estos los mecanismos de seguridad para aplicaciones específicas en servidores por ejemplo a través de FTP y Telnet.

Otros son los circuitos a nivel de pasarela que aplica mecanismos de seguridad cuando se establece la conexión TCP o UDP.

Otro tipo de firewall es el de capa de red. Como su nombre indica actúa a nivel de red como si fuese un filtro de los paquetes IP que recibe en cualquiera de sus campos, véase origen o destino por ejemplo, también filtra a nivel de la capa de enlace (MAC) o de transporte (puertos).

También existen cortafuegos en la capa de aplicación por ejemplo comprobar las direcciones de las páginas Web a las que se intenta acceder a través del tráfico http. Estos *firewalls* de tráfico http se suelen denominar Proxy y su función en ocultar las verdaderas direcciones a las que accedemos. Son accesos más controlados.

Finalmente comentar que también existe la posibilidad de crear un cortafuegos casero como si fuera un software más del PC, su función en este caso es filtrar las conexiones entre el PC y la red.

Existen unas políticas de configuración de los cortafuegos, estás pueden ser o políticas restrictivas que rechazan todo el tráfico salvo el que está permitido, es decir, habilitan el

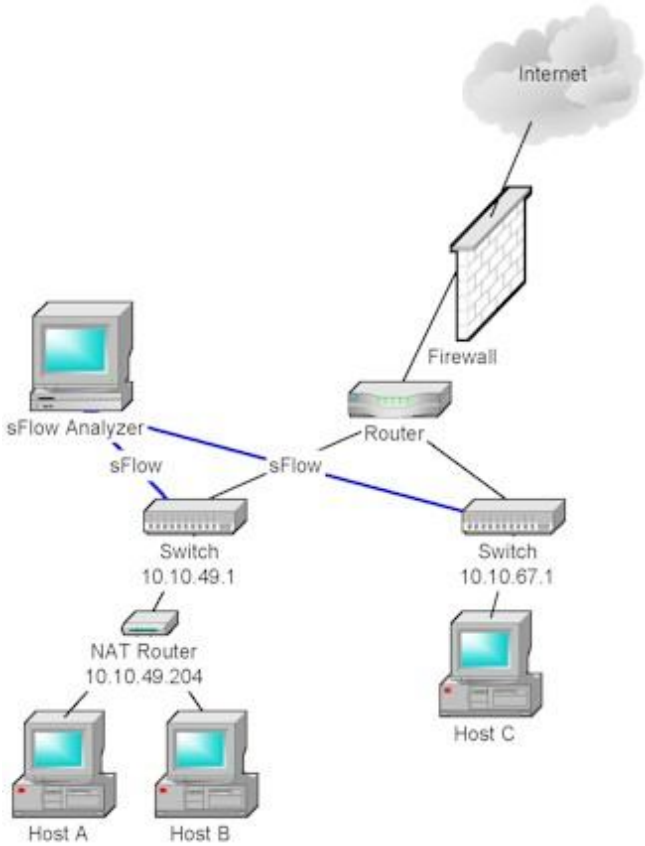
tráfico solo a las personas autorizadas. Y la otra política es la permisiva que es el caso contrario, el tráfico está abierto a todo el que quiera salvo a los que explícitamente se le deniega el acceso.

El punto 3 trata sobre

NAT

Network Address Translation, dice que es una herramienta para esconder el esquema de direccionamiento de red presente detrás de un entorno de servidor de seguridad. Permite abordar un esquema elegido para ser desplegado detrás de un cortafuegos, mientras mantiene la capacidad de conectarse a los recursos externos a través del firewall.

Otras definiciones encontradas en otras fuentes definen NAT como un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.



http://www.sflow.org/detectNAT/images/network.jpg

El punto 4 trata sobre maneras de

CONFIGURACIÓN DEL FIREWALL

Estos se pueden implementar en hardware o software, aunque también se puede hacer combinando ambas formas. Otra operación bastante frecuente es conectar al firewall una zona desmilitarizada, que hace como una tercera red, también llamada DMZ en la que se ubican los servidores que han de estar accesibles desde el exterior. Todas estas acciones con los *firewalls* son necesarias para tener una buena seguridad pero en cualquier caso no son medidas suficientes por lo tanto habrá que abarcar otros ámbitos de la seguridad informática para garantizar una buena seguridad.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

El punto 4 abarca un amplio temario sobre todas estas configuraciones comunes de los *firewalls* desde las configuraciones del servidor de seguridad, explicación exhaustiva de la zona desmilitarizada DMZ incluyendo el DMZ con doble configuración del cortafuegos, los servidores Proxy, y los riesgos controlados por los cortafuegos como los ataques basados en debilidades del software o desbordamiento del búfer entre otros

P8 EVALUACIÓN DE SEGURIDAD, PRUEBAS, ANÁLISIS DE VULNERABILIDADES.

En el punto P8 se trata sobre la evaluación de seguridad, pruebas y análisis de vulnerabilidad. En este caso no todos los puntos son referentes a la auditoría o la seguridad en redes así que están seleccionados algunos de los puntos más importantes.

El punto 3 trata sobre los

TIPOS DE PRUEBAS DE INTROMISIONES Y EVALUACIÓN DE VULNERABILIDADES

3.1.1 Existen varios tipos de pruebas de intromisión que, dependiendo de las circunstancias, afecta al ámbito de la evaluación, la metodología adoptada y los niveles de garantía de la auditoría.

3.1.2 El individuo (caso la administración de TI) responsable de velar por la organización debe evaluar varias alternativas, la selección de la que proporciona el máximo nivel de garantías con el menor daño aceptable para la organización (análisis de costo / riesgo).

3.1.3 Debe haber un acuerdo sobre el tipo de pruebas de intromisión que se llevarán a cabo, ya sean intrusivas o no intrusivas.

El punto 4 trata sobre

PRUEBAS DE EXTERIORES Y EVALUACIÓN DE VULNERABILIDADES

4.1 Internet

4.1.1 La finalidad de las pruebas de Internet es poner en peligro la red de destino. La metodología necesaria para realizar esta prueba permite una comprobación sistemática de las vulnerabilidades conocidas y la búsqueda de posibles riesgos de seguridad. La metodología empleada habitualmente incluye los procesos de:

• Recogida de la información (reconocimiento)

• Red de enumeración

• Análisis de la vulnerabilidad

• Explotación

• Resultados de los análisis e informes

4.1.2 Existen diversas variaciones de los procesos enumerados en la sección 4.1.1. Sin embargo, un común, la escritura normalizada es normalmente seguida y debe proporcionar un método detallado y exacto de la ejecución. Además, la complejidad de las nuevas vulnerabilidades y los métodos de explotación que requieren un estudio detallado con la historia de la información que apoyarse.

Otro punto interesante es el punto 8 que tarta sobre los antecedentes de la tecnología

WIRELESS

8.1 Antecedentes y riesgos asociados a las tecnologías inalámbricas

8.1.1 Con el advenimiento de la tecnología inalámbrica para transmitir datos y voz, los controles instituidos mediante dispositivos perimetrales están desapareciendo. Atrás han quedado los controles de seguridad físicos, tales como guardias de seguridad, cámaras y cerraduras, que resultaron efectivas en la protección de las redes de cable y transmisión de datos. Las vulnerabilidades más graves son:

• Dependencia WEP para el cifrado.

• Que las redes inalámbricas no estén separadas de otras redes.

• Las direcciones MAC.

• Débil o inexistente gestión de claves.

• Los paquetes Beacon que no se han deshabilitado o "activado".

• Contraseñas por defecto / IP

• Evitar la clave WEP débil

•DHCP que se utiliza en las redes WLAN sin protección.

8.1.3 Además, como con otros tipos de tecnologías, la mayor debilidad de la seguridad inalámbrica no es técnico, sino las deficiencias de instalaciones fuera de la caja. El factor humano suele ser el eslabón más débil.

9.

APLICACIÓN WEB

9,1 Manual y automatizada

9.1.1 las pruebas de aplicaciones Web incluyen pruebas manuales y automatizadas del portal como un extraño, sin información de acceso. Esta prueba complementa las pruebas de penetración externa. El objetivo de esta prueba es obtener una comprensión de cómo las personas interactúan con el sistema de acceso a datos sensibles.

9.1.2 Las pruebas adicionales pueden incluir la comprobación del portal Web por una información privilegiada a través de una cuenta de entrada estándar. El objetivo de esta prueba es determinar la facilidad de acceso a la información sensible que no está autorizada por la cuenta de inicio de sesión (es decir, una escalada de privilegios).

9.1.2 Identificación y explotación de las vulnerabilidades se puede lograr mediante el uso de diversas herramientas comerciales y de código abierto evaluación de la vulnerabilidad.

CAPÍTULO IV
ELABORACIÓN DE UNA GUÍA BASADA EN LA ISO/IEC27002:2005

INTRODUCCIÓN GUÍA

A continuación procedemos a la elaboración de una guía para el auditor en la que encontraremos los pasos a seguir para un correcto funcionamiento de la seguridad corporativa.

Según la ISO/IEC 17799 (versión de 2005) ahora 27002 podemos definir los siguientes puntos de partida:

Primeramente unos términos a tener en cuenta:

TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

2.1

asset
Anything that has value to the organization [ISO/IEC13335-1:2004]

2.2

Control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature ' NOTE Control is also used as a synonym for safeguard or countermeasure.

2.3

Guideline
A description that clarifies what should be done and how, to achieve the objectives set out in policies [ISO/IEC 13335-1:2004]

2.4

Information processing facilities
Any information processing system, service or infrastructure, or the physical locations housing them

2.5

Information security
Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

2.6

Information security event

an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO/IEC TR 18044:2004]

2.7

Information security incident

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC TR 18044:2004]

2.8

Policy

Overall intention and direction as formally expressed by management

2.9

Risk

Combination of the probability of an event and its consequence [ISO/IEC Guide 73:2002]

2.10

Risk analysis

Systematic use of information to identify sources and to estimate the risk [ISO/IEC Guide 73:2002]

2.11

Risk assessment

Overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002]

2.12

Risk evaluation

Process of comparing the estimated risk against given risk criteria to determine the significance of the Risk [ISO/IEC Guide 73:2002]

2.13

Risk management

Coordinated activities to direct and control an organization with regard to risk
NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk Communication.
[ISO/IEC Guide 73:2002]

2.14

Risk treatment

Process of selection and implementation of measures to modify risk [ISO/IEC Guide

73:2002]

2.15

Third party \

That person or body that is recognized as being independent of the parties involved, as concerns the
issue in question
[ISO/IEC Guide 2:1996]

2.16

Threat

A potential cause of an unwanted incident, which may result in harm to a system or organization [ISO/IEC 13335-1:2004]

2.17

Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats [ISO/IEC 13335-1:2004]

COMPOSICIÓN

La **ISO/IEC 17799** de 2005 ahora 27002 tiene la siguiente composición:

a) Security Policy (1);

POLÍTICA DE SEGURIDAD

b) Organizing Information Security (2);

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

c) Asset Management (2);

GESTIÓN DE ACTIVOS

d) Human Resources Security (3);

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

e) Physical and Environmental Security (2);

SEGURIDAD FÍSICA Y AMBIENTAL

f) Communications and Operations Management (10);

GESTIÓN DE COMUNICACIONES Y OPERACIONES

g) Access Control (7);

CONTROL DE ACCESO

h) Information Systems Acquisition, Development and Maintenance (6);

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

i) Information Security Incident Management (2);

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

j) Business Continuity Management (1)

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

k) Compliance (3).

CUMPLIMIENTO

De todos estos puntos vamos a detallar y explicar aquellos puntos a seguir por un auditor de sistemas de información para mantener el buen estado en los sistemas de la empresa basados en redes de datos.

GUÍA

5. Security policy

5.1Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

En este punto simplemente se comenta cual es el objetivo de las políticas de seguridad. Se pone como objetivo proporcionar un apoyo a la gestión de seguridad de la información según se haya prescrito en los requisitos previos de los empresarios y de los reglamentos ya existentes.

A continuación se comenta que la gestión debe establecer una política clara, coherente con los objetivos del negocio y demostrar apoyo y compromiso por la seguridad.

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) *a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);*

b) *a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;*

c) *a framework for setting control objectives and controls, including the structure of risk assessment and risk management;*

d) *a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:*

   1) *compliance with legislative, regulatory, and contractual requirements;*

   2) *security education, training, and awareness requirements;*

   3) *business continuity management;*

   4) *consequences of information security policy violations;*

e) *a definition of general and specific responsibilities for information security management, including reporting information security incidents;*

f) *References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.*

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organization, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC 13335-1:2004.

Este punto trata sobre la política de información de seguridad de los documentos. Primeramente describe lo que llama "*Control*" como una aprobación por parte de un comité de seguridad normalmente de un documento de información sobre la política de seguridad que además ha de ser publicado y comunicado a todos los empleados y a las partes interesadas del exterior.

A continuación se detalla una orientación para establecer el documento de política de seguridad.

Este documento debe tener información acerca de:

- Definición de la seguridad de la información detallando
    - Objetivos generales
    - Alcance
    - Importancia de la seguridad para el intercambio de información
- Declaración de intenciones de gestión
    - Apoyo a los objetivos
    - Apoyo a los principios de la seguridad en la estrategia de negocios
- Marco para establecer objetivos de control, estructura de la evaluación del riesgo y gestión de éste.
- Breve explicación de:
    - Principios
    - Normas
    - Requisitos de cumplimiento, incluyendo:
        - Requisitos legales, reglamentarios y contractuales.
        - Educación, Seguridad, Formación, y requisitos de sensibilización.
        - Gestión de continuidad del negocio.
        - Consecuencias de la política de seguridad
- Definición de responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo información sobre los incidentes ocurridos si

los hubiera.

- Referencias a la documentación aportada donde se pueden aportar más políticas, otros sistemas más específicos, y todo lo que sea de ayuda para obtener una mejor calidad de la seguridad de la información para su posterior uso.

Como nota al final del texto nos comunica que estas políticas de seguridad deben ser comunicadas al resto de la empresa y los usuarios más relevantes, siendo ésta, accesible y comprensible para el lector. Estas políticas deberán ser usadas en la realidad por lo tanto deberán estar siempre en un lugar visible para todo miembro de la organización y ser puestas en práctica para un correcto uso de la seguridad de la información de ésta.

5.1.2 Review of the information security policy

Control

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Implementation guidance

The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.

The review of the information security policy should take account of the results of management reviews. There should be defined management review procedures, including a schedule or period of the review.

The input to the management review should include information on:

a) feedback from interested parties;

b) results of independent reviews (see 6.1.8);

c) status of preventive and corrective actions (see 6.1.8 and 15.2.1);

d) results of previous management reviews;

e) process performance and information security policy compliance;

f) changes that could affect the organization's approach to managing

information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;

g) trends related to threats and vulnerabilities;

h) reported information security incidents (see 13.1);

i) recommendations provided by relevant authorities (see 6.1.6).

The output from the management review should include any decisions and actions related to:

a) improvement of the organization's approach to managing information security and its processes;

b) improvement of control objectives and controls;

c) improvement in the allocation of resources and/or responsibilities.

A record of the management review should be maintained. Management approval for the revised policy should be obtained.

En este punto visto a groso modo, lo que se nos viene a decir es que la política de seguridad debe ser revisada en intervalos planificados o cuando se produzcan cambios para poder garantizar que se mantiene su idoneidad, adecuación y eficacia.

A continuación se detalla cómo se hacen los exámenes de gestión para garantizar que las revisiones se realizan adecuadamente.

El punto 9.2 de esta ISO trata sobre la seguridad de los equipos con el objetivo de evitar pérdidas, daños, robos o cualquier situación que ponga en peligro a los equipos físicos y por lo tanto el trabajo normal para la organización.

9. Physical and environmental security

9.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities. Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment sitting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

En esta pequeña parte viene a decir como el equipo ha de estar protegido de posibles amenazas físicas y ambientales.

Esto se refiere a la importancia de salvaguardar las máquinas de posibles efectos adversos sobre ellas. Estos pueden ser producidos por ejemplo por una rotura, robo, o manipulación entre otros. Pongamos por ejemplo el hecho de que hubiera una gotera en la sala de ordenadores y alguna pudiera caer sobre uno de estos. Evidentemente la máquina se perdería junto con la información que hubiera en ésta.

Por otra parte cuando hablamos de daños físicos, perfectamente nos podemos referir a accesos no autorizados a alguna información confidencial, o que se produzca algún daño o pérdida en el equipo con la consiguiente pérdida de información. Sería interesante mantener copias de seguridad de ciertos datos e información importantes en otros lugares de la empresa para poder recurrir a ellas en caso de posibles pérdidas.

Respecto a este punto podemos añadir algunos comentarios sobre Cobit 4.1

En el punto DS12 – Administración del Ambiente Físico – Descripción del proceso.

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de las instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores

ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

OBJETIVOS DE CONTROL

DS12.1 Selección y Diseño del Centro de Datos

Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas de Seguridad Física

Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, la ubicación del equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y resolución de incidentes de seguridad física.

DS12.3 Acceso Físico

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección Contra Factores Ambientales

Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS12.5 Administración de Instalaciones Físicas

Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir el nivel requerido de protección física					C	A/R	C				C
Seleccionar y comisionar el sitio (centro de datos, oficina, etc)	I	C	C	C	C	A/R	C		C	C	C
Implementar medidas de ambiente físico					I	A/R	I	I			C
Administrar el ambiente físico (mantenimiento, monitoreo y reportes incluidos)						A/R	C				
Definir e implementar procesos para mantenimiento y autorización de acceso físico				C	I	A/R	I	I	I		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

www.itgi.org

9.2.1 Equipment siting and protection

Control

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Implementation guidance

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;

b) information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;

c) items requiring special protection should be isolated to reduce the general level of protection required;

d) controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;

a) guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established;

b) environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities;

c) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

h) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;

i) equipment processing sensitive information should be protected to minimize the risk of information leakage due to emanation.

En este punto se comenta el emplazamiento y protección de equipos. El control sobre este punto viene a decir que los equipos deben situarse o protegerse de forma que se reduzcan los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.

A continuación se describen unas directrices para proteger los equipos,

- El equipo estará situado de tal manera que reduzca el número de accesos a las áreas de trabajo.

- Las instalaciones donde haya información importante deberá ser una zona restringida para evitar posibles accesos inadecuados.

- Si hay datos que requieran más protección que los demás estos se aislarán de manera que haya una protección en proporción a los datos que se considere.

- Los controles se adoptarán para evitar daños físicos como robos, incendios, explosivos, humo, agua o vandalismo entre otros.

    - Debe haber unas directrices que controlen temas de no comer, beber o fumar en zonas de procesamiento de datos.
    - Las condiciones ambientales como la temperatura o la humedad deben estar controlados en toda la zona de proceso de datos para salvaguardar las máquinas.
    - Todo esto debe ser aplicado a todos los edificios además de tener en cuenta la instalación de filtros contra rayos o agentes externos en todos los

lugares que se precise.

- La utilización de métodos de protección especiales se deberán considerar como equipamientos de entornos industriales.

- Para equipos de procesamiento de la información especialmente sensible de ser protegida se deberá de minimizar el riesgo de fugas o de emanación.

9.2.2 Supporting utilities

Control
Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation guidance
All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning should be adequate for the systems they are supporting. Support utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans should cover the action to be taken on failure of the UPS. A back-up generator should be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators should be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large, a separate power substation.

Emergency power off switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure.

The water supply should be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from

acting effectively. An alarm system to detect malfunctions in the supporting utilities should be evaluated and installed if required.

Telecommunications equipment should be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services should be adequate to meet local legal requirements for emergency communications.

Other information
Options to achieve continuity of power supplies include multiple feeds to avoid a single point of failure in the power supply.

Este punto trata sobre las instalaciones de suministro. El control trata sobre como los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en instalaciones de los suministros.

Algunos servicios básicos como electricidad, agua, calefacción, ventilación, o aire acondicionado entre otros, deben ser adecuados para los sistemas a los que estén dando servicio. Todos estos servicios deberían ser inspeccionados periódicamente y probado para ver que cumplen correctamente con su servicio. También vienen bien estas revisiones para poder evitar posibles fallos en el futuro.

Además en este punto se nos presenta el plan de contingencia. Este no puede faltar en la organización y es preciso que contenga toda la información necesaria de cómo actuar ante alguna posible crisis en estos aspectos. Tenemos que tener en cuenta cómo actuar en caso de un apagón prolongado, tener un medio donde poder almacenar la información como si de un *Backup* se tratase, aquí llamado Backup-generador. Un suministro adecuado de combustible debe estar disponible para asegurar que el generador pueda utilizarse durante todo el periodo de tiempo que dure el apagón. Los sistemas de alimentación ininterrumpida (UPS) y los generadores, deberán ser chequeados también periódicamente para asegurar su correcto funcionamiento y deberán ser probados con las recomendaciones del fabricante. Además se podrían usar múltiples fuentes de energía y si el sitio fuera grande y con posibilidades, estaría bien tener alguna otra subestación de energía independiente. En caso de poder, esta práctica sería de gran importancia. También debería

haber interruptores de energía por si se diera el caso de una emergencia, y estos deberán estar ubicados cerca de las salidas de emergencia en las salas de los equipos para ganar tiempo. Además deberá haber una luz de emergencia en caso de que falle la alimentación en las máquinas.

El suministro de agua debe ser estable al igual que el suministro del aire acondicionado, equipos de humidificación y extintores. Para evitar cualquier mal funcionamiento de uno de estos deberá haber algún sistema de alarma además de las propias revisiones periódicas. Los equipos de telecomunicaciones deberán poder conectarse con el proveedor de servicios al menos por dos rutas diferentes para evitar que al fallo de una de estas no podamos establecer la comunicación con el mismo en caso de hacer falta. También se deberán cumplimentar los requisitos de servicios de voz con el proveedor cumpliendo los requisitos legales para las comunicaciones en caso de emergencia.

9.2.3 Cabling security

Control
Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Implementation guidance
The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

b) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas;

c) power cables should be segregated from communications cables to prevent interference;

d) clearly identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables;

e) a documented patch list should be used to reduce the possibility of errors;

f) for sensitive or critical systems further controls to consider include:

1) installation of armored conduit and locked rooms or boxes at inspection and termination points;

2) use of alternative routings and/or transmission media providing appropriate security;

3) use of fiber optic cabling;

4) use of electromagnetic shielding to protect the cables;

5) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

6) controlled access to patch panels and cable rooms;

En este punto más cercano a las redes concretamente vamos a hablar de la seguridad del cableado, tema de vital importancia para que se pueda establecer y mantener la comunicación.

Primeramente comentar que el cableado eléctrico y de telecomunicaciones que transmiten datos, voz o que sirven de soporte a los servicios de la información debe estar protegido frente a interceptaciones o daños físicos.

A continuación se nos presenta más detalladamente los siguientes aspectos:

- Las líneas de comunicación deben instalarse en zonas seguras, bajo tierra y con una protección adecuada de todo el cableado.

- Esto debe ser protegido de la intercepción no autorizada o daño, por ejemplo usando un conducto o evitando estar en zonas públicas transitadas.

- Los cables de alimentación deberán estar separados de los cables de datos para

poder evitar así que se produzcan interferencias entre ambos.

- Todo el cableado deberá estar etiquetado y las marcas de los equipos deberán ser usadas para intentar reducir el número de errores por manipulación tal como se produce con el parcheo de cables de red equivocados.

- Se debe elaborar una lista de parches bien documentados que deberá usarse para reducir la posibilidad de errores, para ello también será necesario que estas listas pasen unos controles para asegurar que la información de ésta sea correcta y se aplique adecuadamente.

- Para sistemas críticos se debe considerar lo siguiente:
    - Instalación de conductos blindados y habitaciones cerradas o en cajas de inspección y los puntos de terminación.
    - Uso de rutas alternativas y otros medios de transmisión para más seguridad.
    - Uso de cableado de fibra óptica.
    - Uso de blindaje electromagnético para proteger los cables.
    - Iniciación de técnica de barridos y controles físicos de los dispositivos no autorizados con los cables.
    - Controlar mediante accesos estrictamente autorizados que no se pueda manipular nada del cableado ni de los paneles de conexión de las salas de procesos de datos o de los armarios de red.

10. Communications and operations management

10.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

En este punto 10.2 vamos a tratar el tema de la gestión de prestación de los servicios por terceros.

Este punto se divide en tres a su vez, la prestación de servicios, la supervisión y revisión de los servicios prestados por terceros, y la gestión de cambios en los servicios prestados por terceros. A continuación se detalla cada punto.

10.2.1 Service delivery

Control

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Implementation guidance

Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.

The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 14.1).

En el punto 10.2.1 hablaremos de la prestación de servicios, siendo la idea que se deben comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de prestación, incluidos en el acuerdo de prestación de servicios por terceros, son objeto de implantación, operación y mantenimiento por parte del tercero. A continuación comenta que la prestación de servicios por un tercero debe incluir las medidas de seguridad acordadas, las definiciones de los servicios, y los aspectos de la gestión de servicios acordados. En caso de los acuerdos con empresas externas, la organización debe planificar las fases necesarias para la transición de toda la información, posibles desplazamientos y todas las posibles tareas durante la fase de adaptación, en cualquier caso lo principal será mantener la seguridad durante este periodo. La organización debe asegurarse de que el tercero tiene suficiente capacidad para dar servicio, junto con planes de viabilidad destinados a garantizar la continuidad del servicio acordado aunque se produjesen fallos de servicio o algún desastre inesperado.

10.2.2 Monitoring and review of third party services

Control
The services, reports and records provided by the third party should be regularly monitored and
reviewed, and audits should be carried out regularly.

Implementation guidance
Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This should involve a service management relationship and process between the organization and the third party to:

a) monitor service performance levels to check adherence to the agreements;

b) review service reports produced by the third party and arrange regular progress meetings as required by the agreements;

c) provide information about information security incidents and review of this information by the third party and the organization as required by

the agreements and any supporting guidelines and procedures;

d) *review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;*

e) *resolve and manage any identified problems.*

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the organization should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that requirement of the agreement (see 6.2.3), in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. The organization should ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response through a clearly defined reporting process, format and structure.

Other information

In case of outsourcing, the organization needs to be aware that the ultimate responsibility for information processed by an outsourcing party remains with the organization.

En el punto 10.2.2 vamos a tratar el tema de seguimiento, monitorización y revisión de los servicios prestados por terceros. Los servicios, informes y registro proporcionados por el tercero deben ser objeto de supervisión y revisión periódica, y también deberán de llevarse a cabo auditorías periódicas.

Comentar que el seguimiento y la revisión de los servicios de terceros deben garantizar que las condiciones de seguridad de la información y las condiciones del contrato con los acuerdos a los que se llegara en su día se estén cumpliendo y por lo tanto que los incidentes de seguridad y los problemas que deriven se gestionan adecuadamente.

Debe existir una relación entre la gestión de servicios y los procesos entre la empresa y las terceras partes de tal manera que se pueda cumplir los siguientes aspectos.

- Monitorización para los servicios que se acuerden.

- Informes periódicos de los servicios producidos por terceros y encuentros también periódicos para ver como se cumplen las expectativas.

- Proporcionar información sobre cualquier incidente de seguridad producido y revisión por parte del tercero como por parte de la empresa.

- Exámenes de posibles fallos detectados por auditorías externas y de los registros de eventos de seguridad, problemas operativos o perturbaciones relacionadas con los servicios prestados.

- Resolver y gestionar los problemas identificados.

La responsabilidad de gestionar la relaciones con terceros deberá ser asignado a alguien de la plantilla de la empresa o a un equipo. Además, la empresa deberá controlar que los externos asignan responsabilidades para controles de cumplimiento y la aplicación de los requisitos acordados. Se debe disponer de recursos y conocimientos técnicos suficientes para afrontar que se cumplan los requisitos acordados. Además deben tomarse las medidas adecuadas cuando se observen deficiencias en la prestación de servicios por terceros.

Por otra parte la empresa deberá mantener el control general y deberá tener visibilidad suficiente en todos los aspectos de la seguridad de la información, que sean tanto sensibles como críticos, y poder acceder a las instalaciones de procesamiento de datos procesados o

gestionada por terceros.

Algunas actividades que deben mantenerse visibles para la empresa son: la gestión de cambios, identificación de vulnerabilidades, y la seguridad de la presentación de incidentes tanto como la respuesta a estos a través de un proceso bien definido.

Finalmente se comenta, que en caso de subcontrataciones, la empresa deberá ser consciente de que la responsabilidad final sigue siendo de la propia empresa, consciente de la información procesada en parte por los externos.

10.2.3 Managing changes to third party services

Control
Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Implementation guidance
The process of managing changes to a third party service needs to take account of:

a) changes made by the organization to implement:
   1) enhancements to the current services offered;
   2) development of any new applications and systems;
   3) modifications or updates of the organization's policies and procedures;
   4) new controls to resolve information security incidents and to improve security;

b) changes in third party services to implement:
   1) changes and enhancement to networks;
   2) use of new technologies;
   3) adoption of new products or newer versions/releases;
   4) new development tools and environments;
   5) changes to physical location of service facilities;
   6) change of vendors.

Este punto trata sobre la gestión de cambios en los servicios prestados terceros, el control dice que se deben gestionar los cambios en la prestación de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados y reevaluación de los riesgos.

El proceso de gestión de los cambios de los servicios de terceros debe tener en cuenta:

- Los cambios realizados por la empresa deberán implementar:
  - Mejoras en los servicios actuales ofrecidos.
  - El desarrollo de nuevas aplicaciones y sistemas.
  - Modificaciones o actualizaciones de las políticas de procedimientos.
  - Los controles nuevos para resolver incidentes de seguridad deberán mejorar la misma.
- Los cambios en los servicios de terceros deberán poner en práctica:
  - Cambios y la mejora de las redes.
  - Uso de nuevas tecnologías.
  - Adopción de nuevos productos y versiones.
  - Nuevas herramientas de entorno y desarrollo.
  - Cambios en la ubicación física de las instalaciones.
  - Cambio de proveedores

En este punto podemos hacer algunas referencias de Cobit 4.1.

El punto Entregar y Dar Soporte (DS2) – Administrar los Servicios de Terceros dice que:

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

Los objetivos de control son:

- DS2.1 Identificación de todas las relaciones con proveedores.
- DS2.2 Gestión de relaciones con proveedores.
- DS2.3 Administración de riesgos del proveedor.
- DS2.4 Monitoreo del desempeño del proveedor.

En el primer punto se plantea que se deben identificar todos los servicios que vamos a concertar con los terceros y estos acuerdos se deberán categorizar según los acuerdos con el proveedor, significado y criticidad. Todo esto deberá estar documentado junto con las relaciones técnicas existentes y organizacionales que cubren los roles, responsabilidades, metas, entregas esperadas y credenciales de estos proveedores.

En el segundo básicamente nos dice que hay que formalizar los procesos de gestión de relación con cada proveedor, y explica cómo los dueños de las relaciones *deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en*

la transparencia, por ejemplo a través de SLAs.

El tercer punto habla de que hay que identificar y mitigar posibles riesgos existentes en las relaciones con los terceros y asegurar la continuidad del negocio de forma segura y eficiente. *La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad de los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos.*

El último punto dice que se debe establecer algún proceso para monitorear las prestaciones del servicio para asegurar que se cumple con las prestaciones acordadas y que además sean las más competitivas con los proveedores alternativos.

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Identificar y categorizar las relaciones de los servicios de terceros				I	C	R	C	R	A/R	C	C
Definir y documentar los procesos de administración del proveedor		C		A	I	R	I	R	R	C	C
Establecer políticas y procedimientos de evaluación y suspensión de proveedores		C		A	C	C		C	R	C	C
Identificar, valorar y mitigar los riesgos del proveedor		I		A		R		R	R	C	C
Monitorear la prestación del servicio del proveedor				R	A	R		R	R	C	C
Evaluar las metas de largo plazo de la relación del servicio para todos los interesados	C	C	C	A/R	C	C	C	C	R	C	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

www.itgi.org

10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

El objetivo en este caso será asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

10.6.1 Network controls

Control
Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Implementation guidance
Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) *operational responsibility for networks should be separated from computer operations where appropriate (see 10.1.3);*
b) *responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;*
c) *special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications (see 11.4 and 12.3); special controls may also be required to maintain the availability of the network services and computers connected;*
d) *appropriate logging and monitoring should be applied to enable recording of security relevant actions;*
e) *management activities should be closely co-ordinated both to optimize the service to the organization and to ensure that controls*

are consistently applied across the information processing infrastructure.

En este punto vamos a comentar los controles de red, las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.

Los administradores de red deben aplicar controles para garantizar la seguridad de la información en las redes, y la protección de los servicios conectados de accesos no autorizados. En particular, se debe considerar:

- La responsabilidad operativa de las redes debe estar separada de las operaciones de la máquina.

- Deberán establecerse las responsabilidades y procedimientos para la gestión de equipos en remoto y los de áreas de los usuarios.

- Los controles se deberán establecer para proteger la confidencialidad e integridad de los datos que pasan a través de redes públicas o inalámbricas y también se deberá proteger las aplicaciones. También deberá haber controles para proteger los servicios de red y equipos conectados.

- Deben establecerse procedimientos adecuados de registro y control para permitir las grabaciones de seguridad.

- Las actividades de gestión deberán estar estrechamente coordinadas para

coordinar el servicio como para garantizar que los controles se aplican de una manera coherente en toda la infraestructura.

10.6.2 Security of network services

Control
Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

Implementation guidance
The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information
Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption, and network connection controls;
b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
c) procedures for the network service usage to restrict access to network services or applications, where necessary.

En el punto 10.6.2 hablaremos de la seguridad en los servicios de red. El control en este caso dice que se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de

servicios de red, tanto si se prestan dentro de la organización como si se subcontrata.

Deben ser acordados la capacidad del proveedor de servicios de red para gestionar sus funciones de una forma segura además de controlarse regularmente con auditorías también acordadas.

Las disposiciones de seguridad necesarias para determinados servicios como la revisión de características de seguridad, niveles de servicio, y gestión de requisitos, deben estar identificados.

La organización debe garantizar que los proveedores de servicio de red aplican estas medidas.

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas y redes de valor añadido y soluciones de seguridad de la red tales como *firewalls* y sistemas de detección de intrusos. Estos servicios pueden variar dependiendo del ancho de banda.

Las funciones de seguridad de los servicios de red pueden ser:

- La tecnología aplicada para la seguridad de los servicios de red tales como autenticación, cifrado y controles de conexión en red.

- Los parámetros técnicos necesarios para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión de red.

- Los procedimientos para restringir el acceso a los servicios de red o aplicaciones en caso necesario.

11. Access control

11.4 Network access control

Objective: To prevent unauthorized access to networked services.

Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the network services by ensuring:

a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;

b) appropriate authentication mechanisms are applied for users and equipment;

c) control of user access to information services in enforced.

El objetivo es prevenir el acceso no autorizado a los servicios de red.

En este apartado general se comenta que los accesos de los usuarios a las redes y servicios de redes internos y externos, deben estar controlados.
A su vez, el acceso de estos usuarios tampoco debería comprometer la seguridad de los servicios de red, garantizando en ello que:

- Las interfaces de la red de la organización y de todas aquellas que sean de su propiedad, al igual que las redes públicas sean adecuadas.
- Los mecanismos de autenticación son adecuados para los usuarios y los equipos.
- El control de acceso de usuarios a los servicios en ejecución sea el adecuado.

11.4.1 Policy on use of network services

Control
Users should only be provided with access to the services that they have been specifically authorized to use.

Implementation guidance
A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) *the networks and network services which are allowed to be accessed;*
b) *authorization procedures for determining who is allowed to access which networks and networked services;*
c) *management controls and procedures to protect access to network connections and network services;*
d) *the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).*

The policy on the use of network services should be consistent with the business access control policy (see 11.1).

Other information
Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.

En el punto 11.4.1 hablaremos de las políticas de uso de los servicios de red. El punto de control viene a decir que se debe proporcionar a los usuarios el acceso sólo a los servicios para los que estén autorizados. Las políticas deberán formularse sobre la utilización de las redes y servicios de red.

En estas políticas de deberán incluir los siguientes aspectos:

- Determinar las redes y los servicios de redes accesibles.
- Procedimientos de autenticación para determinar quien accede a las redes y a los servicios de red.
- Controles de mantenimiento y procedimientos para proteger el acceso a las conexiones red y servicios de red.
- Los medios utilizados para permitir el acceso a redes o algún servicio de red.

Finalmente se comenta que la política sobre el uso de servicios de red debe ser compatible con las políticas de control de acceso del negocio.

También que las conexiones no autorizadas pueden afectar a toda la organización. Estos controles son muy importantes para las conexiones de red en negocios con informaciones importantes o para usuarios que estén especialmente expuestos a ataques véase por ejemplo áreas públicas o externas que estén fuera de de la gestión de la seguridad de la empresa.

11.4.2 User authentication for external connections

Control

Appropriate authentication methods should be used to control access by remote users.

Implementation guidance

Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions. Dedicated private lines can also be used to provide assurance of the source of connections.

Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations. When using this control, an organization should not use network services, which include call forwarding, or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. The call back process should ensure that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that the call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility. Cryptographic techniques, e.g. based on machine certificates, can be used for node authentication. This is part of several VPN based solutions.

Additional authentication controls should be implemented to. control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

Other information
External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. This is especially important if the connection uses a network that is outside the control of the organization's security management.

El punto 11.4.2 trata sobre la Autenticación de usuarios para conexiones externas.

El punto de control dice que deben utilizarse los métodos apropiados de autenticación para controlar los accesos en remoto.

La autenticación de los usuarios en remoto se puede lograr usando distintas técnicas, entre éstas, se nombran las basadas en cifrado, *token* de hardware, o protocolos de desafío-respuesta. Algunas de estas técnicas son usadas para la implementación de las VPN (Virtual Private Network - Red Privada Virtual). También se pueden usar Líneas privadas dedicadas para ofrecer garantías de las fuentes de conexión.

Procedimientos Dial-Back (de llamada de retorno). El sistema detecta que quien llama este autorizado y es el propio sistema en encargado de llamar a este al teléfono o dirección que figure en el sistema.

Otros controles, por ejemplo, pueden autenticar a los usuarios tratando de establecer una conexión a la red desde lugares fuera de la oficina, en remoto. Al usar este control, la organización no debe usar los servicios de red que incluyan desvío de llamadas, o si lo hacen debe deshabilitar el uso de estas funciones para evitar el problema asociado con el desvío de llamadas, por ejemplo que se establecieran

desviación de conexiones o llamadas de tal manera que ajenos a la empresa puedan hacer uso de la red de datos para un uso para el cual no está definido, o por ejemplo que se desvíen llamadas de tal forma que otros puedan usar las líneas de comunicación para fines que no son de la organización.

Con las conexiones en general deberemos tener cuidado de que no haya líneas "en escucha", es decir, una línea pinchada por algún sitio. Para que no se produzcan estos hechos se deben establecer controles, por ejemplo verificar si cuando se establece una conexión, se está estableciendo de una manera real entre un extremo y el otro.

Aparte de las redes de conexión por VPN, se nos presentan las redes inalámbricas, en este caso, también se deberán realizar controles de acceso sobre todo porque en este tipo de redes es más fácil que alguien se cuele sin ser captado por la organización además de ser más accesible las capturas de tráfico en la red.

Finalmente se comenta como estás redes de acceso externo son todo un coladero y por lo tanto en estas se deberán intensificar los controles y cuidados para poder mantener la red en un buen estado. Existen diversos métodos para poder autenticarse pero algunos de los más fuertes son los basados en técnicas criptográficas. Es importante determinar a partir de una evaluación de riesgo el nivel de protección requerido, así se podrán aplicar un método u otro. Además habrá que tener especial cuidado con redes que estén fuera del control de seguridad de la organización.

11.4.3 Equipment identification in networks

Control
Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

Implementation guidance
Equipment identification can be used if it is important that the communication can only be initiated from a specific location or equipment. An identifier in or attached to, the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network

the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

Other information
This control can be complemented with other techniques to authenticate the equipment's user (see 11.4.2). Equipment identification can be applied additionally to user authentication.

Este punto 11.4.3 habla sobre la identificación de los equipos en redes, se refiere a que cuando se establecen conexiones exista alguna manera en que en todo momento se sepa qué equipo establece qué comunicación y hacia dónde. Esto se consigue identificando los equipos al autenticarse las conexiones.

En general, este punto lo que viene a decir es que podemos controlar las conexiones de red desde un equipo físico, esto es poder controlar que desde un equipo concreto se pueda acceder a diferentes servicios, es una manera más de controlar los accesos.
Solo estarán autorizados ciertos equipos para acceder a ciertos sitios.

Este tipo de control también puede estar complementado con otras técnicas de las anteriores, es una manera de controlar por una parte al usuario y por otra al equipo.

11.4.4 Remote diagnostic and configuration port protection

Control
Physical and logical access to diagnostic and configuration ports should be controlled.

Implementation guidance
Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

Ports, services, and similar facilities installed on a computer or network facility, which is not specifically required for business functionality, should be disabled or removed.

Other information
Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.

Este punto trata sobre el diagnóstico remoto y protección de los puertos de configuración.

El control comenta que se controlará el acceso físico y lógico a los puertos de diagnóstico y configuración. Se deben realizar controles para el acceso a los puertos de configuración de diagnóstico e incluir el uso de un bloqueo de teclas y apoyo a los procedimientos para controlar el acceso físico a un puerto. Véase por ejemplo un procedimiento consistente en asegurar que los puertos de diagnóstico y configuración sólo se pueden acceder mediante acuerdo entre el director de servicios informáticos y el HW/SW que requiere el personal para el acceso.

Puertos, servicios, centros e instalaciones similares instaladas en un equipo o instalación de red que no se requiere específicamente para la funcionalidad empresarial, deben ser desactivados y/o eliminados.

Muchos sistemas informáticos, sistemas de red o sistemas de comunicación, se instalan como un control remoto de diagnóstico por los ingenieros de mantenimiento. Si estos puertos no se protegen, proporcionan un medio de acceso no autorizado lo cual se debe evitar.

11.4.5 Segregation in networks

Control
Groups of information services, users, and information systems should be segregated on networks.

Implementation guidance

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical network domains to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

Such a network perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (see 11.4.6 and 11.4.7) and to block unauthorized access in accordance with the organization's access control policy (see 11.1). An example of this type of gateway is what is commonly referred to as a firewall. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the organization.

Networks can also be segregated using the network device functionality, e.g. IP switching. Separate domains can then be implemented by controlling the network data flows using the routing/switching capabilities, such as access control lists.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 10.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (see 11.4.6 and 11.4.7).

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

Other information

Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to existing information systems that use the network, some of which may require protection from other network users because of their sensitivity or criticality.

El punto 11.4.5 trata sobre la segregación en redes. El control viene a decir que los grupos de servicios de información, usuarios, y sistemas de información deben estar segregados en redes.

Existe un método de control de la seguridad de grandes redes que es dividirlas en distintos dominios de red externa, cada uno protegido por un perímetro de seguridad definida. Un conjunto de controles puede ser aplicado en distintos dominios de la red lógica para poder llevar a cabo la división. Los dominios deben ser definidos en base a una evaluación de riesgos y los requisitos de seguridad diferentes en cada uno de los dominios.

Estos perímetros de red pueden ser implementados cuando se realiza la pasarela segura entre dos redes y así controlas el acceso y flujo de datos entre dominios. Estas puertas de enlace deben filtrar el tráfico para bloquear accesos no autorizados según conste en la política de control de accesos para la organización.

También pone explícitamente que este tipo de puerta de enlace se conoce comúnmente como un servidor de seguridad.

Otros métodos de segregación de distintos dominios lógicos es restringir el acceso a la red mediante el uso de redes privadas virtuales para distintos grupos de usuarios dentro de la organización.

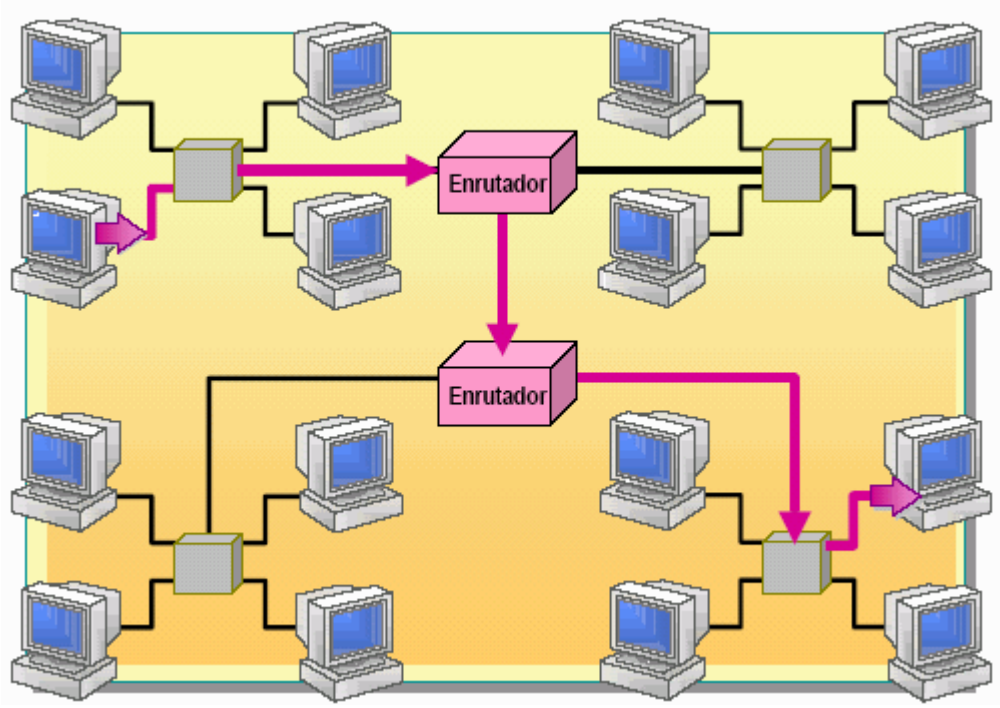
Las redes también pueden ser separadas utilizando la funcionalidad de dispositivos de red como por ejemplo los conmutadores IP. Dominios independientes pueden ponerse en práctica mediante el control de los flujos de datos de la red mediante el enrutamiento, capacidades de conmutación tales como las listas de control de acceso.

Los criterios de segregación de las redes en dominios se debe basar en la política de requisitos y control de acceso, también debe tener en cuenta el costo y la repercusión en el rendimiento debidos a la incorporación enrutamientos de la red y la tecnología adecuada de las puertas de enlace.

Además de todo esto, la segregación de las redes debe basarse en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o las líneas de negocio, con el fin de reducir el impacto total de una interrupción en el servicio.

Debería tenerse en cuenta la segregación de redes inalámbricas internas y privadas. Como los perímetros de estas redes no estén bien definidos, la evaluación del riesgo deberá llevarse a cabo para identificar los controles a los que se deba proceder, como autenticaciones más estrictas, uso de más método de criptografía entre otras.

Finalmente se comenta que pueden existir redes que se deban extender fuera de las fronteras de la organización. Éstas conllevan otros riesgos por los cuales también se deberán realizar controles teniendo en cuenta su criticidad.



http://www.monografias.com/trabajos30/conceptos-redes/Image1396.gif

11.4.6 Network connection control

Control

For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

Implementation guidance

*The network access rights of users should be maintained and updated as required by the access control policy (see 11.1.1**).**The connection capability of users can be restricted through network gateways that filter traffic by means of pre-defined tables or rules. Examples of applications to which restrictions should be applied are:*

a) messaging, e.g. electronic mail;

b) file transfer;

c) interactive access;

d) application access,

Linking network access rights to certain times of day or dates should be considered.

Other information
The incorporation of controls to restrict the connection capability of the users may be required by the access control policy for shared networks, especially those extending across organizational boundaries.

En el punto 11.4.6 vamos a hablar del control de las conexiones a la red. En un primer punto se dice que en redes compartidas especialmente las que estén fuera de la empresa y en consonancia con la política de control de acceso y los requisitos de las aplicaciones del negocio, deben restringirse para los usuarios que quieran conectarse a éstas.
Los derechos de los usuarios de acceso a la red deben mantenerse y actualizarse cuando sea necesario por la política de control de acceso. La capacidad de conexión de los usuarios puede ser restringidos a través de pasarelas de red que filtren el tráfico por medio de tablas predefinidas o reglas.

Ejemplos de aplicaciones en que las restricciones deben aplicarse son los siguientes:

- Servicios de mensajería como correo electrónico.
- Transferencia de archivos
- Accesos interactivos
- Acceso a aplicaciones
- Vinculación de los derechos de acceso de red a determinadas fechas o horas del día

Finalmente se comenta que la incorporación de controles para restringir la capacidad de conexión de usuarios puede ser requerido por la política de control de acceso a través de redes compartidas, especialmente las que se extienden a través de fronteras organizativas.

11.4.7 Network routing control

Control
Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Implementation guidance
Routing controls should be based on positive source and destination address checking mechanisms.

Security gateways can be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies are employed. Implementers should be aware of the strength and shortcomings of any mechanisms deployed. The requirements for network routing control should be based on the access control policy (see 11.1).

Other information

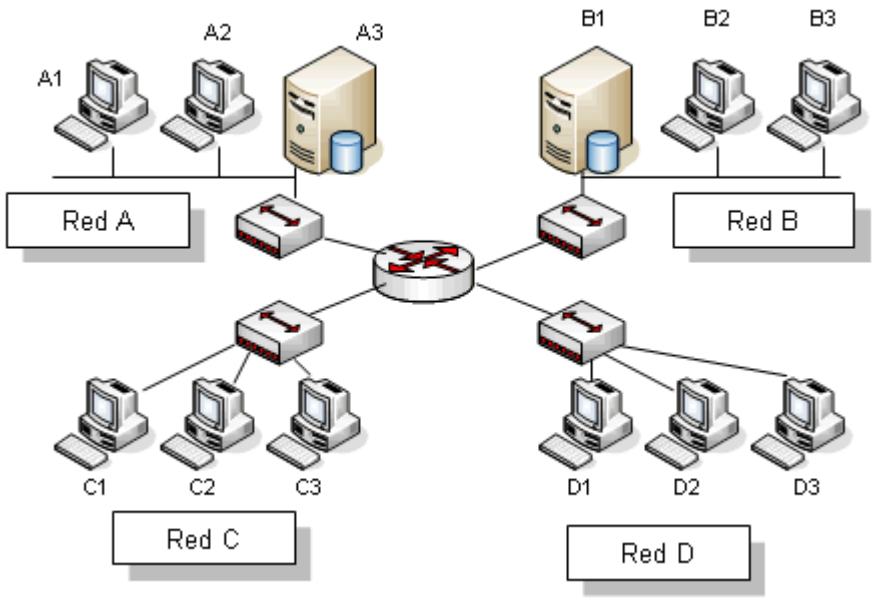
Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (non- organization) users.

En este último punto del apartado 11.4, el 11.4.7, aborda el Control del encadenamiento a la red, primeramente se define en el control que se debe implementar controles de encaminamiento de red (*routing*) para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones del negocio.

Los controles de enrutamiento deben basarse en la dirección de los mecanismos de control de destino. Los *gateways* pueden ser utilizados para validar las direcciones de origen y destino en los puntos de control internos y externos de la red si se utilizan *proxies* y/o dirección de las tecnologías de redes de traducción. Los que realicen las implementaciones deben ser conscientes de la fuerza y las deficiencias de los

mecanismos desplegados. Los requisitos para el control de enrutamiento de red deben basarse en la política de control de acceso.

Finalmente comentar que las redes compartidas y las que se extienden fuera de las fronteras requieren controles de enrutamiento adicionales. Esto se aplica especialmente cuando las redes son compartidas con terceros.



http://www.adrformacion.com/udsimg/wserver/2/img02008.gif

11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

El objetivo de este punto que trata sobre ordenadores portátiles y el teletrabajo se basa en garantizar la seguridad de la información cuando se utilizan estos ordenadores y los servicios de teletrabajo.

11.7.1 Mobile computing and communications

Control

A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

Implementation guidance

When using mobile computing and communicating facilities, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised. The mobile computing policy should take into account the risks of working with mobile computing equipment in unprotected environments.

The mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques (see 12.3).

Users of mobile computing facilities in public places should take care to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date (see 10.4).

Back-ups of critical business information should be taken regularly. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place (see 11.4).

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of the mobile computing facilities. Equipment carrying important, sensitive, and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment (see 9.2.5).

Training should be arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

Other information
Mobile network wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are

a) some wireless security protocols are immature and have known weaknesses;

b) information stored on mobile computers may not be backed-up because of limited network bandwidth and/or because mobile equipment may not be connected at the times when back-ups are scheduled.

El punto 11.7.1 abarca el tema de los portátiles y comunicaciones móviles. El control dice que se debe implementar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.

Cuando se utiliza la informática móvil y las instalaciones de comunicaciones, véase *notebooks, palmtops*, portátiles, tarjetas inteligentes o teléfonos móviles, se debe tener especial cuidado para asegurar que la información comercial no se vea comprometida. La política de informática móvil en entornos desprotegidos. Esta política debe incluir los requisitos de protección física, controles de acceso, técnicas de cifrado, *backups*, y protección antivirus entre otros.

También deberá incluir las reglas y consejos sobre la conexión de dispositivos móviles a las redes y orientación sobre el uso de estas instalaciones en lugares públicos. Se debe tener cuidado al utilizar estos dispositivos en lugares públicos, salas de reuniones, y otras áreas protegidas fuera de la organización. La información almacenada debe estar en un lugar seguro y protegido para evitar posibles accesos indeseados además de estar procesada por servicios por ejemplo de criptografía.

Estos usuarios de los dispositivos de informática móvil en lugares públicos debe tener cuidado para evitar el riesgo de que se cuelen personas no autorizadas. Se pueden y deben llevar a cabo procedimientos contra software malicioso, estos deberían mantenerse actualizados para evitar posibles fuentes de infección debido a las continuas amenazas.

Además de esto se deberán realizar copias de seguridad periódicas. El equipo debe estar disponible para permitir realizar estas copias de manera rápida y sencilla. Una vez realizadas las copias deberán ser llevadas a un lugar seguro para evitar robos o perdidas de información.

Para los dispositivos móviles conectados a redes se debe mantener una protección adecuada, por ejemplo los accesos en remoto a la información a través de la red pública deben poder tener lugar después de haberse logado con éxito y haber pasado unos controles de acceso adecuados.

Al igual que estos dispositivos móviles están protegidos de manera lógica, estos se deben proteger de manera física, daños físicos pueden ser por ejemplo robos en vehículos, otros transportes, hoteles, centros de conferencias, o lugares de reunión.

Se deben establecer procedimientos para garantizar la seguridad en estos dispositivos móviles. Por ejemplo, si la información que se maneja es importante, es posible guardar en un lugar seguro el dispositivo o usar cerraduras especiales para los equipos. Se debe formar a los miembros de la organización sobre la importancia de mantener este tipo de seguridad, y se debe ir adaptando a las necesidades y departamentos, a su vez se debe de formar a los trabajadores sobre que controles deben aplicarse para uso de estos dispositivos.

Finalmente comenta que las conexiones de red inalámbrica en móviles son similares a otros tipos de conexiones de red, pero tienen algunas diferencias importantes que deben tenerse en cuanta para determinar los controles, algunas diferencias típicas son:

- Algunos protocolos de seguridad inalámbrica son inmaduros y tienen carencias conocidas.
- La información almacenada en los equipos móviles no pueden ser respaldados por la red por ancho de banda limitado y/o por que los equipos móviles no se

pueden conectar en los momentos que se está haciendo el *backup.*

11.7.2 Teleworking

Control
A policy, operational plans and procedures should be developed and implemented for teleworking activities.

Implementation guidance
Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy.

Suitable protection of the teleworking site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. Teleworking activities should both be authorized and controlled by management, and it should be ensured that suitable arrangements are in place for this way of working.

The following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;

d) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

e) the use of home networks and requirements or restrictions on the configuration of wireless network services;

f) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

g) access to privately owned equipment (to check the security of the machine or during an investigation), which may be prevented by legislation;

h) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees, contractors or third party users;

i) anti-virus protection and firewall requirements.

The guidelines and arrangements to be considered should include:

a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;

g) the provision of insurance;

h) the procedures for back-up and business continuity;

i) audit and security monitoring;

j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information
Teleworking uses communications technology to enable personnel to work remotely from a fixed location outside of their organization.

Este punto abarca todo lo que es el tema de teletrabajo. Podría verse el teletrabajo como trabajar desde fuera de la organización, ciertamente en el mundo de la informática, especialmente redes y sistemas, el trabajo es claramente en remoto, puede hacer falta estar presente en la organización para algunos temas puntuales, por ejemplo en sistemas si hiciera falta dar algún botonazo a un servidor, o cambiar las cintas del robot del *backup*. En el caso de redes puede hace falta estar presente para cablear armarios de red o instalación de *switches*. Todos estos son temas concretos, pero para llevar lo que sería toda la administración, no haría falta estar presente en la empresa. De ahí surge el teletrabajo. Trabajar desde fuera haciendo lo mismo que desde dentro.

El control pone que se debe redactar e implementar una política de actividades de teletrabajo, así como planes y procedimientos de operación correspondientes.

Seguidamente explica que, las organizaciones deben autorizar actividades de teletrabajo si se consideran que las medidas de seguridad son adecuadas y los controles se cumplan según lo establecido en la política de seguridad de la empresa.
Al igual que en casi todos los casos anteriores hay que controlar la seguridad ante robo, divulgación de información no autorizada, accesos no deseados en remoto, tanto a los sistemas internos de la empresa como al mal uso de las instalaciones.
Por lo tanto las actividades de teletrabajo deben ser autorizadas y controladas por la gerencia, y debe garantizarse que las disposiciones del lugar son adecuadas para trabajar. Se debe considerar:

- La seguridad física existente de la obra, el edificio, y el medio ambiente del lugar en el que se va a realizar el teletrabajo.
- El entorno físico propuesto para desarrollar el teletrabajo.
- Los requisitos de seguridad de las comunicaciones teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la empresa, la sensibilidad de la información a la que se puede acceder pasando por el enlace de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a la información o recursos de otras personas utilizando por ejemplo cuentas de amigos y/o familiares.
- El uso de redes domesticas y requisitos o restricciones a la configuración de los servicios de red inalámbrica.
- Políticas y procedimientos para evitar controversias relativas a los derechos de la propiedad intelectual desarrollada en el equipo de propiedad privada.
- El acceso a los equipos de propiedad privada para comprobar la seguridad de la maquina o durante la investigación, que pueden ser prevenidas por la legislación.
- Los contratos de concesión de licencias de software que son tales que las organizaciones pueden llegar a ser responsables de la concesión de licencias para

el software de cliente en las estaciones de trabajo de propiedad privada de los empleados, contratistas o terceros usuarios.

- La protección anti-virus y los requisitos del servidor de seguridad.

Las directrices y disposiciones para ser considerados deben incluir:

- El suministro del equipo adecuado, instalaciones para el teletrabajo, donde el uso del equipo de propiedad privada no esté bajo el control de la organización no está permitido.
- La definición del trabajo permitido, las horas de trabajo, clasificación de la información que pueda llevarse a cabo en los sistemas internos y servicios en que el teletrabajador está autorizado a acceder.
- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto.
- La seguridad física
- Las normas y orientación sobre los posibles accesos de familiares y visitantes.
- La provisión de HW y SW de mantenimiento.
- La provisión de seguros.
- Los procedimientos de copias de seguridad y continuidad del negocio.
- Auditorías y control de seguridad
- La revocación de la autoridad y los derechos de acceso, y devolución del equipo cuando se termine el periodo o actividades del teletrabajo.

Finalmente se dice que el teletrabajo utiliza la tecnología de comunicaciones que permita al personal trabajar de forma remota desde una ubicación fija fuera de su organización.

12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

Este Nuevo punto habla sobre los controles criptográficos. El objetivo es proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.

12.3.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Implementation guidance

When developing a cryptographic policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected (see also 5.1.1);

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required;

c) the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;

d) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities, e.g. who is responsible for:

1) the implementation of the policy;

2) the key management, including key generation (see also 12.3.2);

f) the standards to be adopted for the effective implementation throughout the organization (which solution is used for which

business processes);

g) *the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).*

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see also 15.1.6).

Cryptographic controls can be used to achieve different security objectives, e.g.:

a) *confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;*

b) *integrity/authenticity: using digital signatures or message authentication codes to protect ' the authenticity and integrity of stored or transmitted sensitive or critical information;*

c) *non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non- occurrence of an event or action.*

Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When using digital signatures, consideration should be given to any relevant legislation, in particular legislation describing the conditions under which a digital signature is legally binding (see 15.1).

Specialist advice should be sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support the implementation of a secure key management system (see also 12.3.2).

ISO/IEC JTC1 SC27 has developed several standards related to cryptographic ***controls.*** *Further information can also be found in IEEE P1363 and the OECD Guidelines on Cryptography.*

El punto 12.3.1 trata sobre la política sobre el uso de controles criptográficos.

El control comenta que una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada y puesto en práctica.

En el desarrollo de una política de cifrado se debe considerar:

- El enfoque de gestión hacia el uso de controles criptográficos en toda la organización.
- Basándose en una evaluación del riesgo, el nivel necesario debe ser fijado teniendo en cuenta la fuerza y la calidad del algoritmo de cifrado requerido.
- Debe hacerse uso de cifrado para la protección de la información crítica que sea transportada en dispositivos móviles o extraíbles.
- El enfoque de la gestión de claves, incluidos los métodos para hacer frente a la protección de claves criptográficas y la recuperación de la información codificada en caso de pérdida.
- Las funciones y responsabilidades de:
    - La aplicación de la política.
    - La gestión y generación de claves.
- Las normas que deben adoptarse para la aplicación por parte de la organización
- El impacto del uso de la información codificada en los controles que dependen de la inspección de contenidos.

Cuando se aplica la política criptográfica en la organización, se debe considerar las regulaciones y restricciones nacionales que podrían aplicarse a la utilización de técnicas criptográficas en el mundo y los problemas de flujo transfronterizo de la información codificada.

Los controles criptográficos se pueden utilizar para alcanzar distintos objetivos de seguridad, por ejemplo:

- Confidencialidad, usando el cifrado de la información para proteger la información sensible o critica, ya sea almacenada o transmitida.
- La integridad / autenticidad, usando firmas digitales o códigos de autenticación.
- El no repudio, uso de técnicas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

Finalmente comentar que tomar decisiones sobre el uso de técnicas criptográficas debe ser visto como una parte del proceso de evaluación de riesgos y selección de controles.

Esta evaluación puede ser utilizada para determinar si un control criptográfico es adecuado, que tipo de control se puede aplicar, con que propósito y en que procesos del negocio.

Una política sobre el uso de controles es necesaria para maximizar beneficios y minimizar los riesgos de utilización de técnicas criptográficas, y evitar un uso inadecuado o incorrecto. Con el uso de forma digital, se debe considerar la legislación vigente que será lo que de vigor a la firma pues así consta.

12.3.2 Key management

Control
Key management should be in place to support the organization's use of cryptographic techniques.

Implementation guidance
All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used ***to*** *generate, store and archive keys should be physically protected.*

A key management system should be based on an agreed set of standards, procedures, and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) generating and obtaining public key certificates;

c) distributing keys to intended users, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;

i) archiving keys, e.g. for information archived or backed up;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 6.2.3).

<u>Other information</u>
The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770 provides further information on key management. The two types of cryptographic techniques are:

a) secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information; this key has to be kept secret since anyone having access to the key is able to decrypt all information being encrypted with that key, or to introduce unauthorized information using the key;

b) public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret); public key techniques can be used for encryption and to

produce digital signatures (see also ISO/IEC 9796 and ISO/IEC 14888).

There is a threat of forging a digital signature by replacing a user's public key. This problem is addressed by the use of a public key certificate.

Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

Finalmente tenemos el punto 12.3.2 que trata sobre la gestión de claves, el control dice que debe existir un sistema de gestión de claves que admita el uso de técnicas criptográficas por parte de la organización.

Todas las claves criptográficas deben ser protegidas contra toda alteración, perdida, y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no autorizada. Debe existir un equipo que sea utilizado para generar, almacenar y archivar claves que deben estar físicamente protegidas.

Un sistema de gestión de claves debe estar basado en un conjunto de normas, procedimientos, y métodos seguros para:

- Generar claves para distintos sistemas criptográficos y diferentes aplicaciones.
- Generar y obtener certificados de clave pública
- Distribución de claves a los usuarios previstos, incluyendo cómo las claves deben ser activadas cuando las reciban.
- El almacenamiento de las claves, incluyendo cómo los usuarios autorizados pueden acceder a su clave.
- Cambiar o actualizar claves incluyendo las reglas sobre cuándo deben ser cambiadas y como realizarlo.
- Tratar las claves comprometidas.
- Revocar las claves incluyendo como de deben retirar o desactivar.

- La recuperación de claves que se han perdido o dañado, como parte de la gestión de la continuidad del negocio, por ejemplo recuperación de información codificada.
- La información archivada o copias de seguridad.
- La destrucción de las claves.
- El registro y la auditoría de la gestión de actividades relacionadas.

Con el fin de reducir riesgos, se puede proceder a la activación y desactivación de las claves en determinadas fechas, se puede habilitar que sólo estén activas las claves en cuestión durante ese determinado periodo de tiempo. Este periodo debe depender de las circunstancias en que el control de cifrado se use y el riesgo percibido. Además de gestionar la seguridad de claves secretas y privadas, la autenticidad de las claves públicas también deben ser consideradas. Este proceso de autenticación se puede realizar utilizando certificados de clave pública que normalmente son expedidos por una autoridad de certificación que debe ser una organización reconocida con controles adecuados y procedimientos para proporcionar el grado necesario de confianza.

El contenido de los acuerdos de nivel de servicio o contratos con los proveedores externos de servicios de criptografía, por ejemplo una autoridad de certificación, debería abarcar cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta para la prestación de los servicios.

La gestión de claves criptográficas es esencial para el uso eficaz de técnicas criptográficas. Hay dos tipos de técnicas:

- Las de clave secreta, cuando dos o más partes comparten una misma clave y ésta se utiliza tanto para cifrar como para descifrar. Esta clave debe ser mantenida en secreto para que nadie tenga acceso a la información cifrada ya sea para descifrarla o para introducir información falsa.
- Técnicas de clave pública, donde cada usuario tiene un par de claves, una pública, y una privada.

Existen amenazas de falsificar una forma digital mediante la sustitución de la clave pública del usuario. Este problema se aborda con el uso de certificados de clave pública.
Las técnicas criptográficas también pueden ser usadas para proteger las propias claves. Se pueden usar procedimientos para tramitar solicitudes legales de acceso a claves criptográficas.

RELACIÓN COBIT CON ASPECTOS DE LA GUÍA

DS5 – Garantizar la Seguridad de los Sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

OBJETIVOS DE CONTROL

DS5 Garantizar la Seguridad de los Sistemas

DS5.1 Administración de la Seguridad de TI

Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que la seguridad este en línea con los requerimientos del negocio.

DS5.2 Plan de Seguridad de TI

Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura y la cultura de seguridad. Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

DS5.3 Administración de Identidad

Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente

para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, Vigilancia y Monitoreo de Seguridad

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

DS5.6 Definición de Incidente de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

DS5.7 Protección de la Tecnología de Seguridad

Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

DS5.8 Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, Detección y Corrección de Software Malicioso

Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).

DS5.10 Seguridad de la Red

Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de Datos Sensitivos

Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

MODELO DE MADUREZ

DS5 Garantizar la Seguridad de los Sistemas

La administración del proceso de Garantizar la seguridad de los sistemas que satisfaga el requerimiento de negocio de TI de mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad es:

***0 No Existente** cuando*

La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

***1 Inicial / Ad Hoc** cuando*

La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

***2 Repetible pero Intuitivo** cuando*

Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad está fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de

herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La habilitación sobre seguridad está disponible

pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

***3 Definido** cuando*

Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio

contra intrusos). Existe habilitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

***4 Administrado y Medible** cuando*

Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de

seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La habilitación sobre seguridad se imparte tanto para TI como para el negocio. La habilitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPls ya están definidos pero no se miden aún.

5 Optimizado *cuando*

La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua.

En la página:
http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=54909

Podemos encontrar un documento interesante que relaciona algunas de las buenas prácticas definidas anteriormente. Concretamente relaciona Cobit 4.1 con ISO 27002 y con ITIL v.3.

De esta guía podemos destacar el punto 5 que describe lo que estas prácticas ofrecen en tres apartados, uno para cada tipo de documento, primeramente Cobit, luego ITIL y finalmente ISO.

Y también podemos resaltar el punto 6 que trata sobre cómo es la mejor manera de implementar Cobit, ITIL e ISO. Es un enfoque bastante general de las buenas prácticas si bien es verdad que acerca del tema de comunicaciones sólo trata algunos puntos como la contratación de servicios a terceros.

RELACIÓN COBIT, ITIL, E ISO/IEC 27002

6. How Best to Implement Cobit, ITIL and ISO/IEC 27002

There is no doubt that effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities. Adoption of standards and best practices enables quick implementation of good procedures and avoids lengthy delays in creating new approaches when reinventing wheels and agreeing on approaches.

However, the best practices adopted have to be consistent with a risk management and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea; their effectiveness depends on how they have been implemented and kept up to date.

They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures.

To ensure policies and procedures are effectively utilised, change enablement is required so management and staff understand what to do, how to do it and why it is important.

For best practices to be effective, the use of a common language and a standardised approach oriented toward real business requirements is best, as it ensures that everyone follows the same set of objectives, issues and priorities.

Tailoring

Every enterprise needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three guidance documents can play a very useful part—Cobit and ISO/IEC 27002 helping to define what

should be done and ITIL providing the how for service management aspects. Typical uses for these standards and practices are:

• To support governance by:
– Providing a management policy and control framework
– Enabling process ownership, clear responsibility and accountability for IT activities
– Aligning IT objectives with business objectives, setting priorities and allocating resources
– Ensuring return on investments and optimising costs
– Making sure that significant risks have been identified and are transparent to management, responsibility for risk management has been assigned and embedded in the organisation, and assurance has been provided to management that effective controls are in place
– Ensuring that resources have been organised efficiently and sufficient capability (technical infrastructure, process and skills) exists to execute the IT strategy
– Making sure that critical IT activities can be monitored and measured, so problems can be identified and corrective action can be taken
• To define requirements in service and project definitions, internally and with service providers, for example:
– Setting clear, business-related IT objectives and metrics
– Defining services and projects in end-user terms
– Creating service level agreements and contracts that can be monitored by customers
– Making sure customer requirements have been cascaded down appropriately into technical IT operational requirements
– Considering services and project portfolios collectively so that relative priorities can be set and resources can be allocated on an equitable and achievable basis

• To verify provider capability or demonstrate competence to the market by:
– Independent third-party assessments and audits
– Contractual commitments
– Attestations and certifications

• To facilitate continuous improvement by:

– Maturity assessments

– Gap analyses

– Benchmarking

– Improvement planning

– Avoidance of re-inventing already proven good approaches

• As a framework for audit/assessment and an external view through:

– Objective and mutually understood criteria

– Benchmarking to justify weaknesses and gaps in control

– Increasing the depth and value of recommendations by following generally accepted preferred approaches

Prioritising

To avoid costly and unfocused implementations of standards and best practices, enterprises need to prioritise where and how to use standards and practices. The enterprise needs an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction that management should follow. The board should:

• Make sure IT is on the board agenda

• Challenge management's activities with regard to IT to make sure that IT issues are uncovered

• Guide management by helping align IT initiatives with real business needs and ensure that management appreciates the potential impact on the business of IT-related risks

• Insist that IT performance be measured and reported to the board

• Establish an IT steering group or IT governing council with responsibility for communicating IT issues between the board and management

• Insist that there be a management framework for IT governance based on a common approach (e.g., CobiT) and a best practice framework for IT service management and security based on a global, de facto standard (e.g., ITIL and ISO/IEC 27002)

Planning

With this mandate and direction in place, management then can initiate and put into action an implementation approach. To help management decide where to begin and to ensure that the implementation process delivers positive results where they are needed most, the following steps are suggested, based on ITGI's IT Governance Implementation Guide:

1. Set up an organisational framework (ideally as part of an overall IT governance initiative) with clear responsibilities and objectives and participation from all interested parties who will take implementation forward and own it as an initiative.

2. Align IT strategy with business goals. In which current business objectives does IT have a significant contribution?

Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT.

CobiT's management guidelines (specifically the goals and metrics) help define IT objectives. Used in conjunction with ITIL, services and service level agreements (SLAs) can be defined in end-user terms.

3. Understand and define the risks. Given the business objectives, what are the risks relating to IT's ability to deliver against these objectives? Consider:

– Previous history and patterns of performance

– Current IT organisational factors

– Complexity and size/scope of the existing or planned IT environment

– Inherent vulnerability of the current and planned IT environment

– Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes.

CobiT's process for risk management (PO9) and the application of the CobiT control framework and information criteria help ensure that risks are identified and owned. Instituting ITIL clarifies operational risks and ISO/IEC 27002 clarifies security risks.

4. Define target areas and identify the process areas in IT that are critical to delivering value and managing these risk areas. The CobiT process framework can be used as the basis, underpinned by ITIL's definition of key service delivery processes and ISO/IEC 27002's security objectives. OGC's publication Management of Risk: Guidance to Practitioner can also be of assistance in assessing and managing risks at any of the four main levels, i.e., strategic, programme, project or operational.

5. Analyse current capability, and identify gaps. Perform a maturity capability assessment to find out where improvements are needed most. The CobiT maturity models provide a basis supported in more detail by ITIL and ISO/IEC 27002 best practices.

6. Develop improvement strategies, and decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies. Specific improvement projects as part of a continuous improvement initiative should be outlined.
The CobiT control objectives and control practices can be supported by more detailed ITIL and ISO/IEC 27002 guidance.

7. Measure results, establish a scorecard mechanism for measuring current performance and monitor the results of new improvements considering, as a minimum, the following key questions:
– Will the organisational structures support strategy implementation?
– Are responsibilities for risk management embedded in the organisation?
– Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
– Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?
CobiT's goals and metrics and ITIL's seven-stage continual improvement approach can form the basis of a scorecard.

8. Repeat steps 2 through 7 on a regular basis.

Avoiding Pitfalls

There are also some obvious, but pragmatic, rules that management ought to follow:

• Treat the implementation initiative as a project activity with a series of phases rather than a 'one-off' step.

• Remember that implementation involves cultural change as well as new processes. Therefore, a key success factor is the enablement and motivation of these changes.

• Make sure there is a clear understanding of the objectives.

• Manage expectations. In most enterprises, achieving successful oversight of IT takes time and is a continuous improvement process.

• Focus first on where it is easiest to make changes and deliver improvements, and build from there one step at a time.

• Obtain top management buy-in and ownership. This needs to be based on the principles of best managing the IT investment.7

• Avoid the initiative becoming perceived as a purely bureaucratic exercise.

• Avoid the unfocused checklist approach.

Aligning Best Practices

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. CobiT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organisation generically. Specific practices and standards such as ITIL and ISO/IEC 27002 cover discrete areas and can be mapped to the CobiT framework, thus providing a hierarchy of guidance materials.

To better understand mapping amongst ITIL, ISO/IEC 27002 and CobiT, refer to appendix I, where each of the CobiT 34 IT processes and control objectives has been mapped to specific sections of ITIL and ISO/IEC 27002; appendix II, where a reverse mapping shows how ITIL V3 key topics map to CobiT 4.1; and appendix III, where a reverse mapping shows how ISO/IEC 27002 classifications map to CobiT. These mappings are based on subjective judgement and are intended only to be a guide.

OGC and ITGI will continue to update ITIL and CobiT including further alignment of their concepts, terminology and content with those of other practices to facilitate easier integration.

CAPÍTULO V
CUESTIONARIO

INTRODUCCIÓN AL CUESTIONARIO

Este cuestionario está basado sobre la ISO/IEC 27002:2005

A lo largo de este proyecto hemos elaborado una guía basada en unos puntos concretos de esta ISO, y sobre dichos puntos está elaborado el cuestionario. Los puntos son los siguientes:

5 - POLÍTICAS DE SEGURIDAD.

9.2 - SEGURIDAD DE LOS EQUIPOS:

- 9.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE LOS EQUIPOS.
- 9.2.2 INSTALACIONES DE SUMINISTRO.
- 9.2.3 SEGURIDAD DEL CABLEADO.

10.2 – GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS:

- 10.2.1 PROVISION DE SERVICIOS.
- 10.2.2 SUPERVISIÓN Y REVISIÓN DE LOS SERVICIOS PRESTADOS POR TERCEROS
- 10.2.3 GESTIÓN DE CAMBIOS EN LOS SERVICIOS PRESATADOS POR TERCEROS.

10.6 - GESTIÓN DE LA SEGURIDAD DE LAS REDES:

- 10.6.1 CONTROLES DE RED.
- 10.6.2 SEGURIDAD DE LOS SERVICIOS DE RED.

11.4 - CONTROL DE ACCESO A LA RED:

- 11.4.1 POLÍTICA DE USO DE LOS SERVICIOS DE RED.
- 11.4.2 AUTENTICACIÓN DE USUARIOS PARA SERVICIOS DE RED.
- 11.4.3 IDENTIFICACIÓN DE EQUIPOS EN LAS REDES.
- 11.4.4 DIAGNÓSTICO REMOTO Y PROTECCIÓN EN LOS PUERTOS DE CONFIGURACIÓN.
- 11.4.5 SEGREGACIÓN DE LAS REDES.
- 11.4.6 CONTROL DE LA CONEXIÓN A LA RED.
- 11.4.7 CONTROL DE ENCAMINAMIENTO DE RED.

11.7 - ORDENADORES PORTÁTILES Y TELETRABAJO:

11.7.1 ORDENADORES PORTÁTILES Y COMUNICACIONES MÓVILES.

11.7.2 TELETRABAJO.

12.3 – CONTROLES CRIPTOGRÁFICOS:

12.3.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS.

12.3.2 GESTIÓN DE CLAVES.

Sobre todos estos puntos podríamos elaborar diversos tipos de cuestionarios más o menos exhaustivos, a continuación se exponen unas preguntas sobre las que se va a elaborar una aplicación en Delphi. Es un ejemplo de cuestionario para poder elaborar una auditoría en una empresa, se expondrá un resultado según sean las respuestas y será este el que implique si se ha pasado la auditoría o no.

Las preguntas de dicho cuestionario son las siguientes, es un caso bastante básico.

PREGUNTAS CUESTIONARIO

1.- ¿Existe un documento de políticas de seguridad de la organización donde consta: la definición de la seguridad en la empresa, la declaración de intenciones de objetivos, marco con los objetivos de control y explicación de términos generales sobre la política empresarial, así como las responsabilidades del personal y las referencias de la documentación aportada?

2.- ¿Se revisan periódicamente las políticas de seguridad de la información para su actualización y mantenimiento?

3.- ¿Todo el personal de la empresa tiene acceso y conoce las políticas expuestas en el documento?

4.- ¿Los equipos están protegidos sobre posibles amenazas físicas y ambientales?

5.- ¿Existen unas instalaciones de suministro adecuadas ante posibles cortes de luz o pérdidas de información ante posibles acontecimientos inesperados?

6.- ¿Está el cableado debidamente protegido, etiquetado y en instalaciones adecuadas?

7.- ¿Los controles de seguridad, la definición de servicios y los niveles de prestación incluidos en el acuerdo de prestación de servicios por terceros son objeto de implantación y mantenimiento por el tercero?

8.- ¿El seguimiento, y la revisión de los servicios gestionados por terceros garantizan que se cumple la seguridad de la información y los acuerdos del contrato?

9.- ¿Se procura hacer mejoras continuas sobre las prestaciones de los servicios incluyendo el mantenimiento y mejoras de las políticas?

10.- ¿Se aplican controles para garantizar la seguridad de la información en redes y la protección sobre accesos no autorizados?

11.- ¿Es acordada la capacidad de los proveedores de servicios de red para gestionar sus funciones de una forma segura además de controlarse mediante auditorías acordadas?

12.- ¿Existen unas políticas de seguridad sobre los servicios de red?, ¿Son llevadas a cabo?

13.- ¿Están implantados unos métodos de autenticación lo suficientemente buenos que garantizan la seguridad de la información ante intentos de accesos no autorizados tanto en oficina como en remoto?

14.- ¿Hay implantado algún método que controle por una parte al trabajador y por otra al equipo?, ¿Desde ciertos equipos sólo se puede acceder a aplicaciones concretas?

15.- ¿Están debidamente protegidos los accesos a puertos que puedan ser conflictivos?

16.- ¿Existen unos criterios en el tema de segregación de redes en dominios, basados en las políticas, requisitos y control de acceso?

17.- ¿Los derechos de los usuarios sobre el acceso a la red se mantienen y actualizan? ¿Se usan pasarelas de red que filtren el tráfico por medio de reglas definidas?

18.- ¿Existen unos mecanismos para controlar el enrutamiento de la red?

19.- ¿Se lleva un control sobre el uso de portátiles y dispositivos móviles?, ¿el uso de estos dispositivos de telecomunicaciones cumplen con las condiciones de seguridad establecidos en las políticas de empresa?

20.- ¿En el tema de teletrabajo, dichas actividades son autorizadas y controladas por la gerencia y se garantiza que las disposiciones del lugar son adecuadas para trabajar?

21.- ¿Existe una política sobre el uso de los controles criptográficos para la protección de la información y es puesta en práctica?

22.- ¿Existe un sistema de gestión de claves basado en un conjunto de normas, procedimientos y método seguros que admita el uso de técnicas criptográficas por parte de la empresa?

EXPLICACIÓN CUESTIONARIO

Después de la exposición de las preguntas continúo explicando cómo se ha llevado a cabo la aplicación y ciertas connotaciones sobre la misma.

El cuestionario consta de una parte inicial basada en los pesos que queremos otorgar a cada pregunta según quiera cada empresa dependiendo del sector al que se dedique. Estos pesos ponderan así las preguntas que podrán tener un valor comprendido entre cero y nueve. Siendo cero de muy poca importancia y los valores crecientes de mayor importancia. Estos valores son orientativos para empresa. Por ejemplo en las pruebas realizadas se han usado un valor de uno para poca importancia, dos para importancia media y tres para preguntas más importantes. Los valores con los que se han realizado las pruebas se han dejado como valores por defecto.

Una vez se han configurado los pesos ya se puede empezar el cuestionario, este consta de veintidós preguntas.

Para hacer una división entre las preguntas se ha procedido a hacer cinco bloques, dos de ellos con sub-bloques o parte I y II respectivamente.

El bloque I es el de las políticas de seguridad, este bloque consta de tres preguntas.

El bloque II es el de seguridad física y ambiental que también cuenta con tres preguntas.

El bloque III es el de gestión de las comunicaciones y operaciones. Este a su vez está dividido en dos partes o sub-bloques. El primero de ellos es la de gestión de la provisión por servicios de terceros que consta de tres preguntas. Y la segunda parte es la gestión de la seguridad de las redes que consta de dos preguntas.

El bloque IV por su parte es el de control de acceso, uno de los puntos fuertes de esta auditoría y se divide también en dos partes, la primera de ellas es el control de acceso a la red con cuatro preguntas en una pantalla y otras tres en otra pantalla. Y la segunda parte es la de ordenadores portátiles y teletrabajo que está formada por dos preguntas.

Finalmente el Bloque V es el de adquisición, desarrollo y mantenimiento de los sistemas de información, este compuesto por dos preguntas.

Por una parte están los pesos de las preguntas que irán a gusto del consumidor. Por la otra parte está la valoración de las respuestas, en este caso valoran de uno a cinco, siendo uno muy mal hasta muy bien que vale cinco.

Finalmente y tras unas sencillas operaciones podremos ver el resultado final. Durante el cuestionario nos podremos desplazar por las pantallas hacia adelante o hacia atrás por si queremos cambiar alguna de las respuestas de pantallas anteriores. Para ello existen unos botones en las pantallas con Anterior y Siguiente y Salir. También se puede navegar por las pantallas con Alt-A para el anterior o Alt-S para la siguiente.

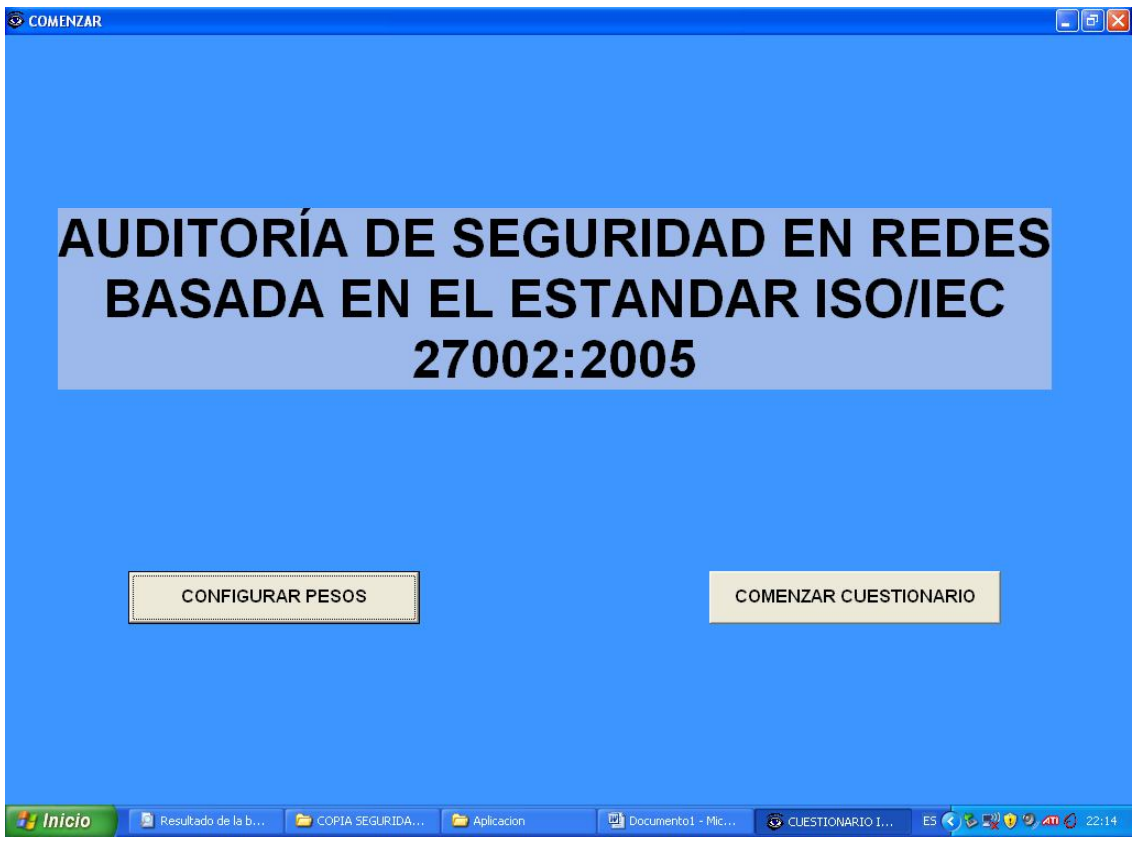
Así mismo si por alguna razón nos dejamos alguna respuesta sin marcar, se lanzará un mensaje de error en la pantalla para poder proseguir navegando por las pantallas.

Cuando se ha terminado de responder a todas las preguntas se nos presenta una pantalla en la que podemos elegir ver los resultados parciales, estos se refieren a los resultados por bloques para saber donde habría que hacer mejoras o un mayor hincapié. Y por otra parte podemos ver también el resultado final en el que saldrá un valor numérico y se expondrá un texto para saber si la auditoría ha pasado con éxito o no.

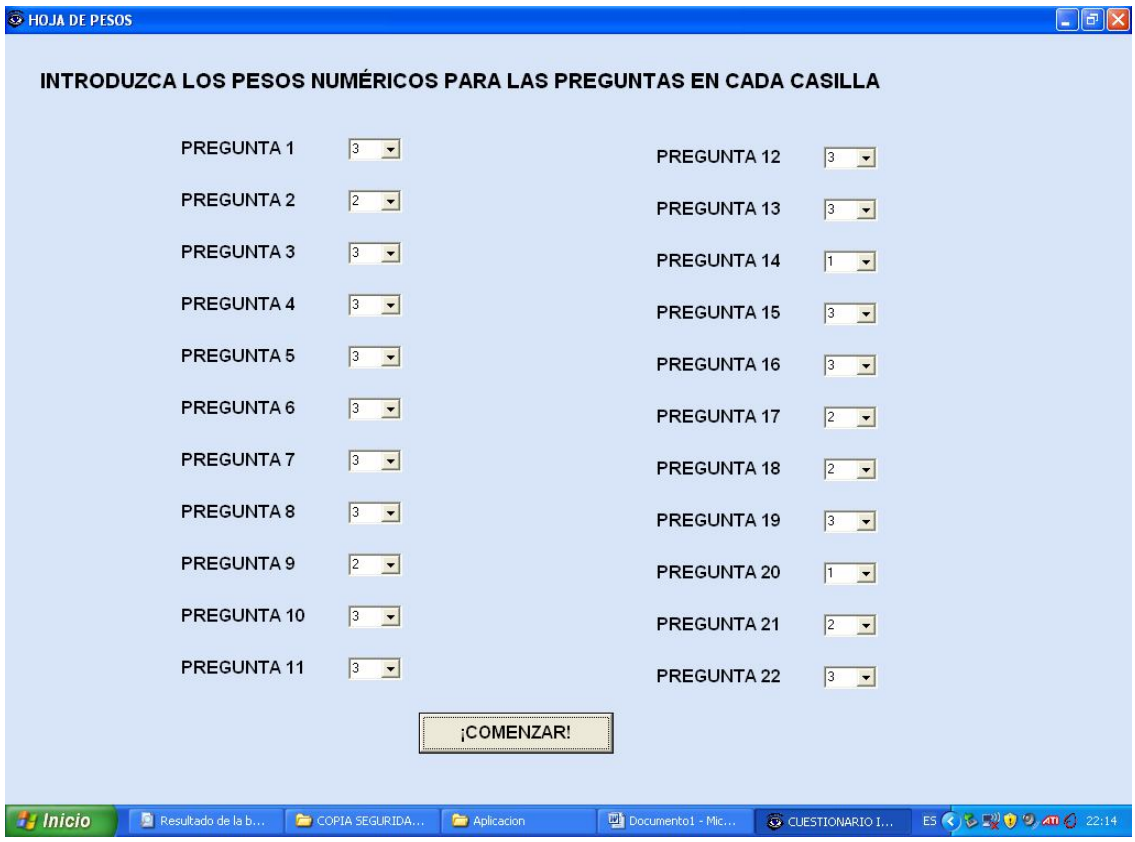
También existe un botón para poder ver las gráficas con los resultados obtenidos por bloques. En esta ventana aparecen tres gráficas. Una para los resultados totales en los bloques en conjunto y otras dos gráficas que muestran el valor total y el valor por cada bloque respectivamente con una señal, asterisco para la primera y una raya para la segunda para ver si ha pasado o no la auditoría y con qué margen.

A su vez será posible la navegación por estas pantallas, es decir, pasar desde la pantalla de resultados parciales al global o gráficas y viceversa.

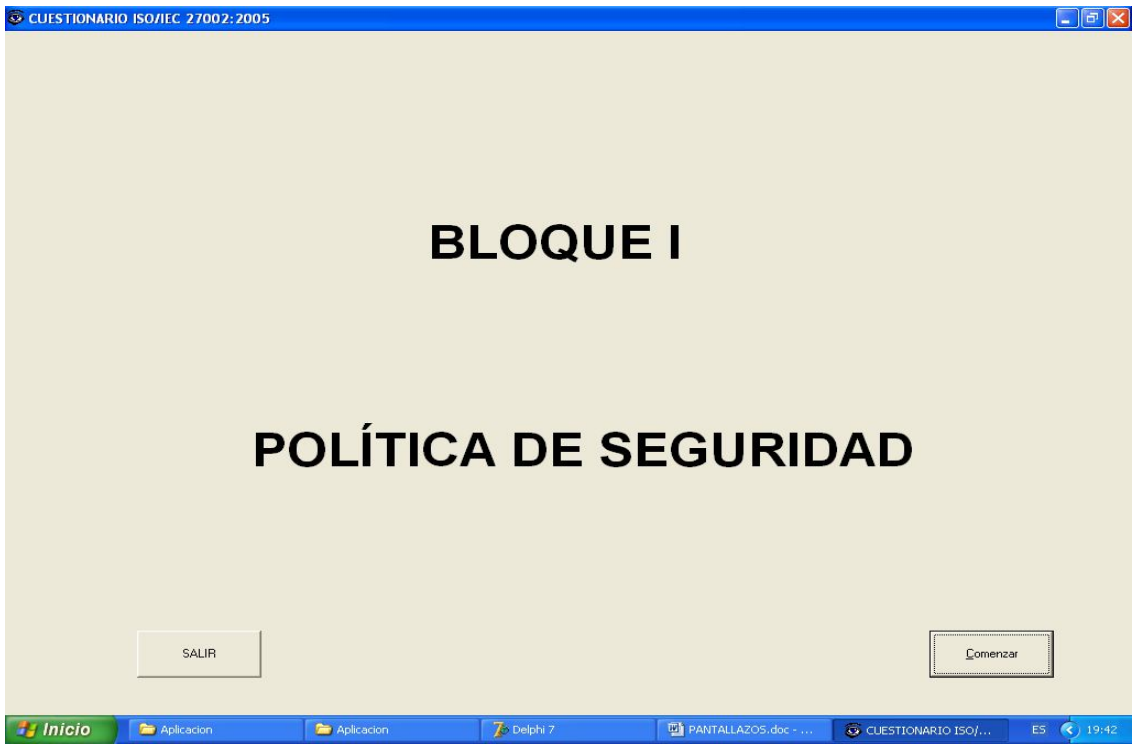
PANTALLAS DE LA APLICACIÓN



Ésta es la pantalla de presentación del cuestionario. Se pueden tomar dos acciones, por una parte configurar los pesos de las preguntas como se dijo anteriormente y si no se desea cambiar los pesos de las preguntas estas se evaluaran con los valores por defecto.

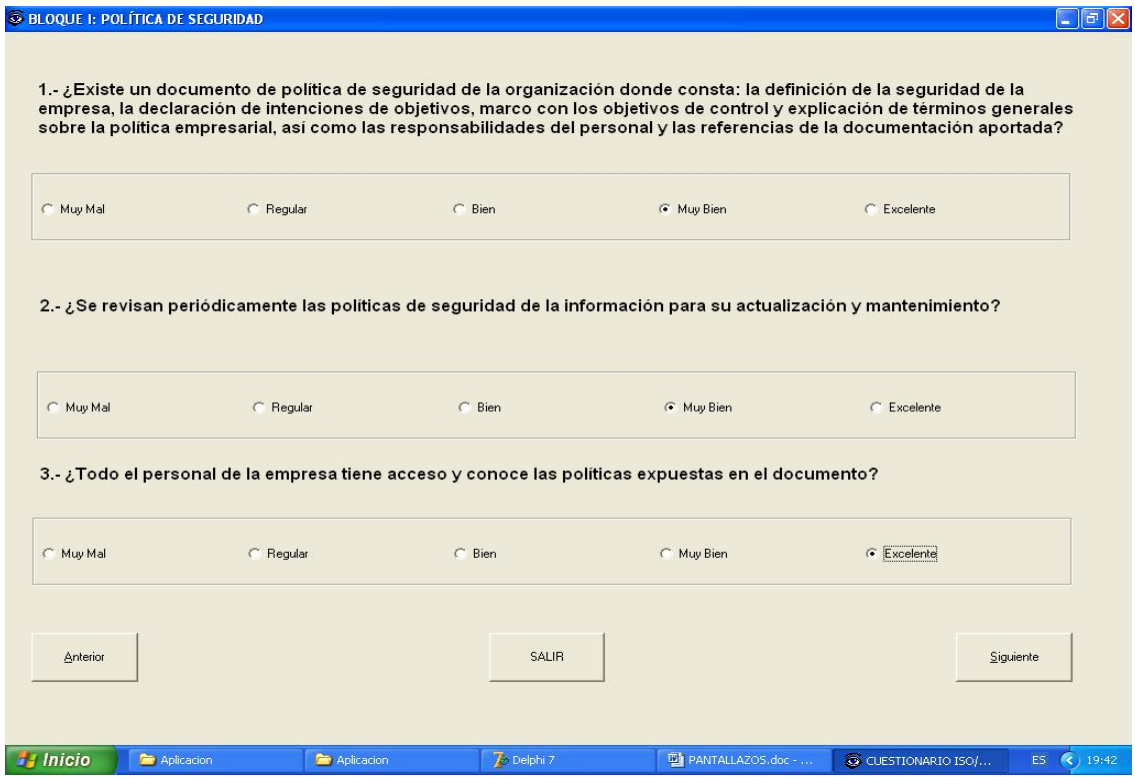


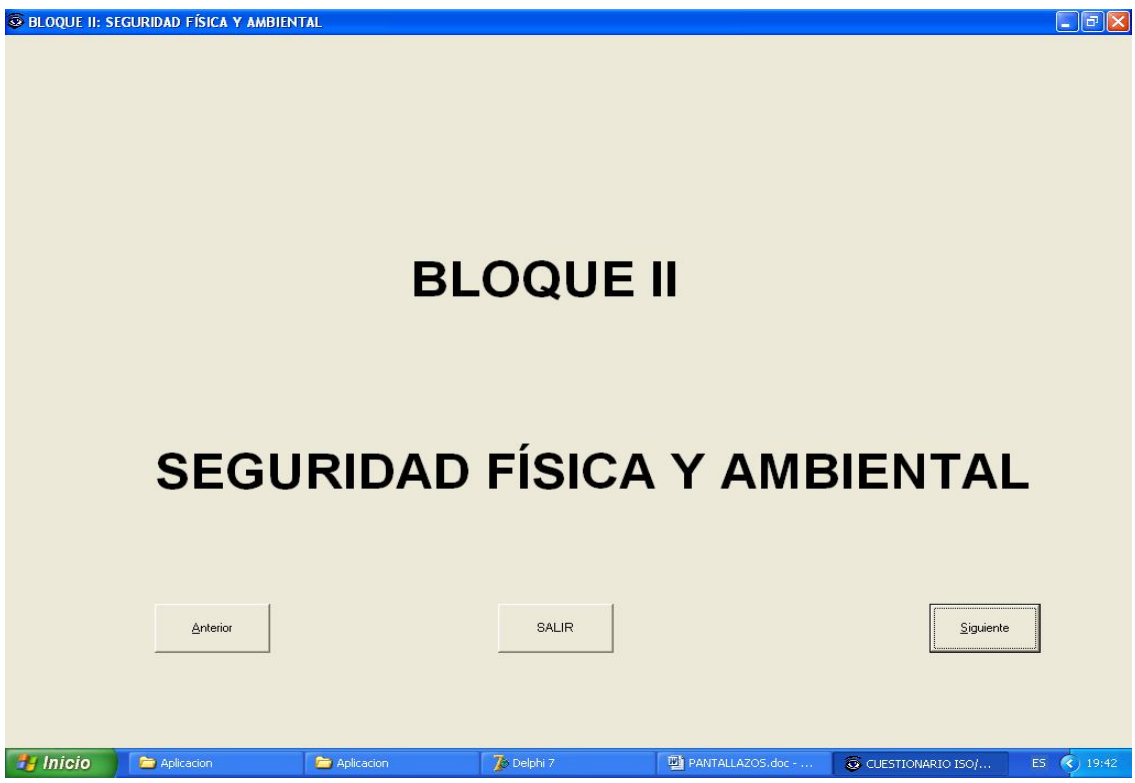
Si optamos por dejar los pesos por defecto podemos pasar directamente a comenzar cuestionario.

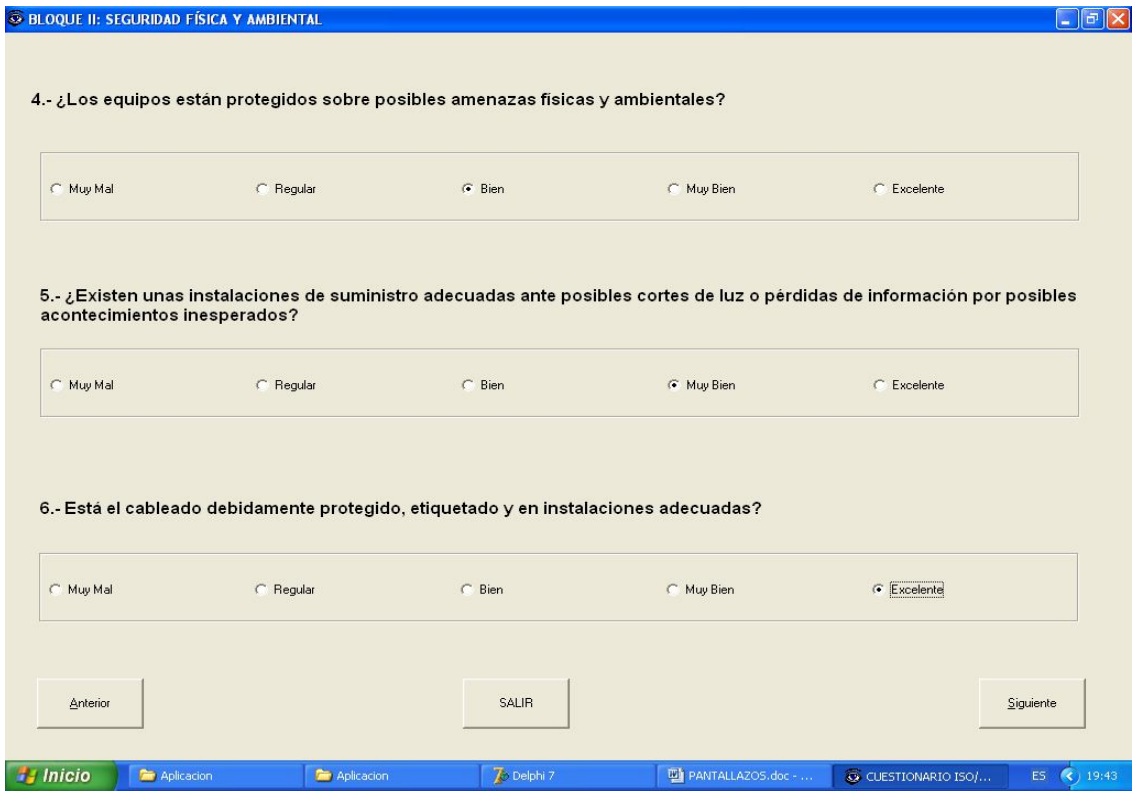


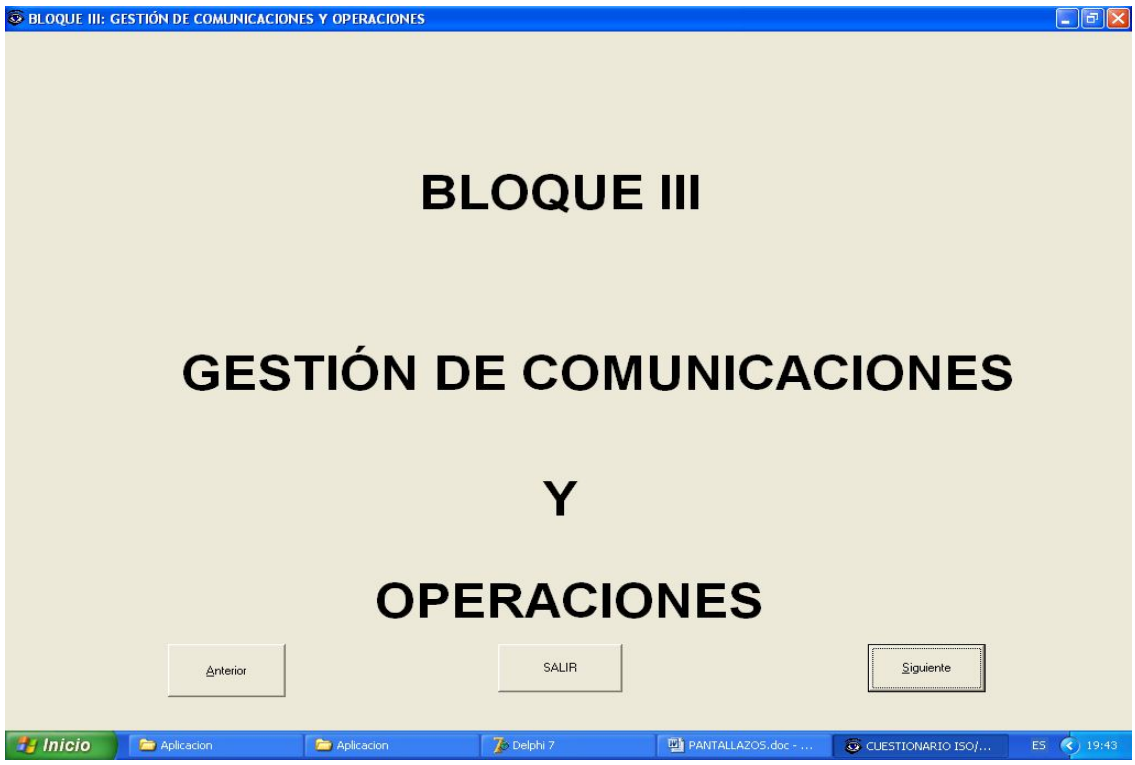
Ahora se muestran las pantallas con las preguntas por bloques.

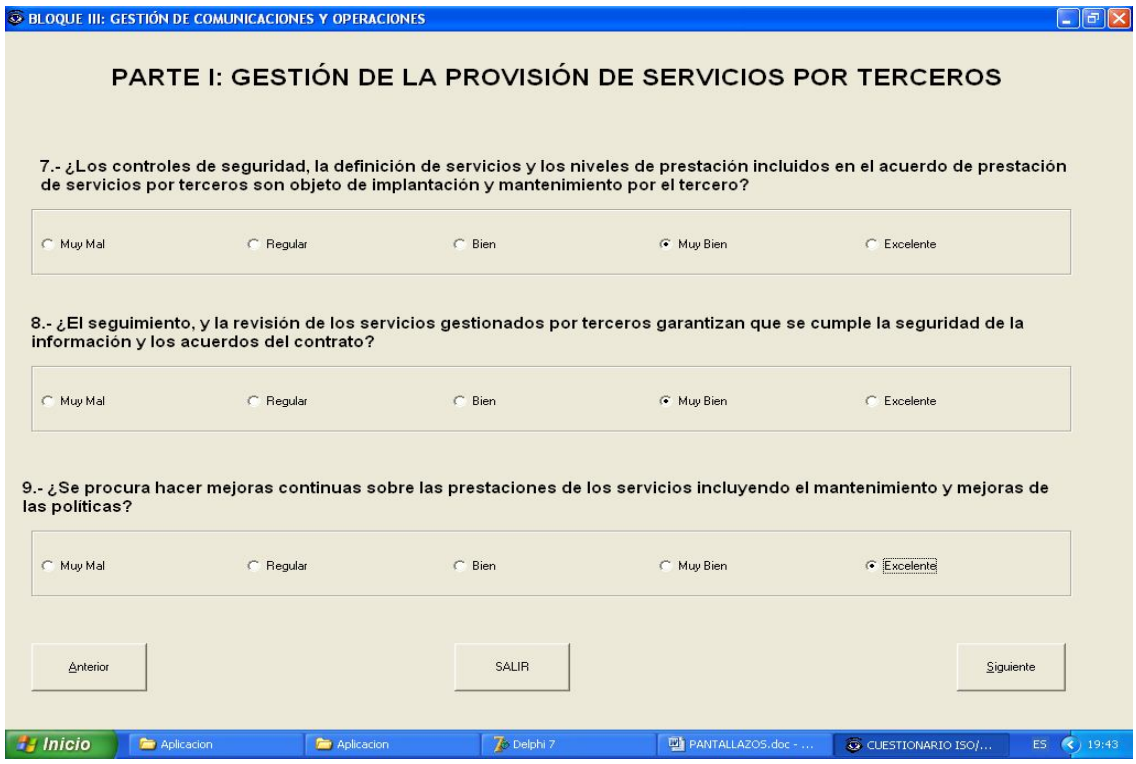
Primeramente se muestran resultados para una auditoría que pasa con éxito.

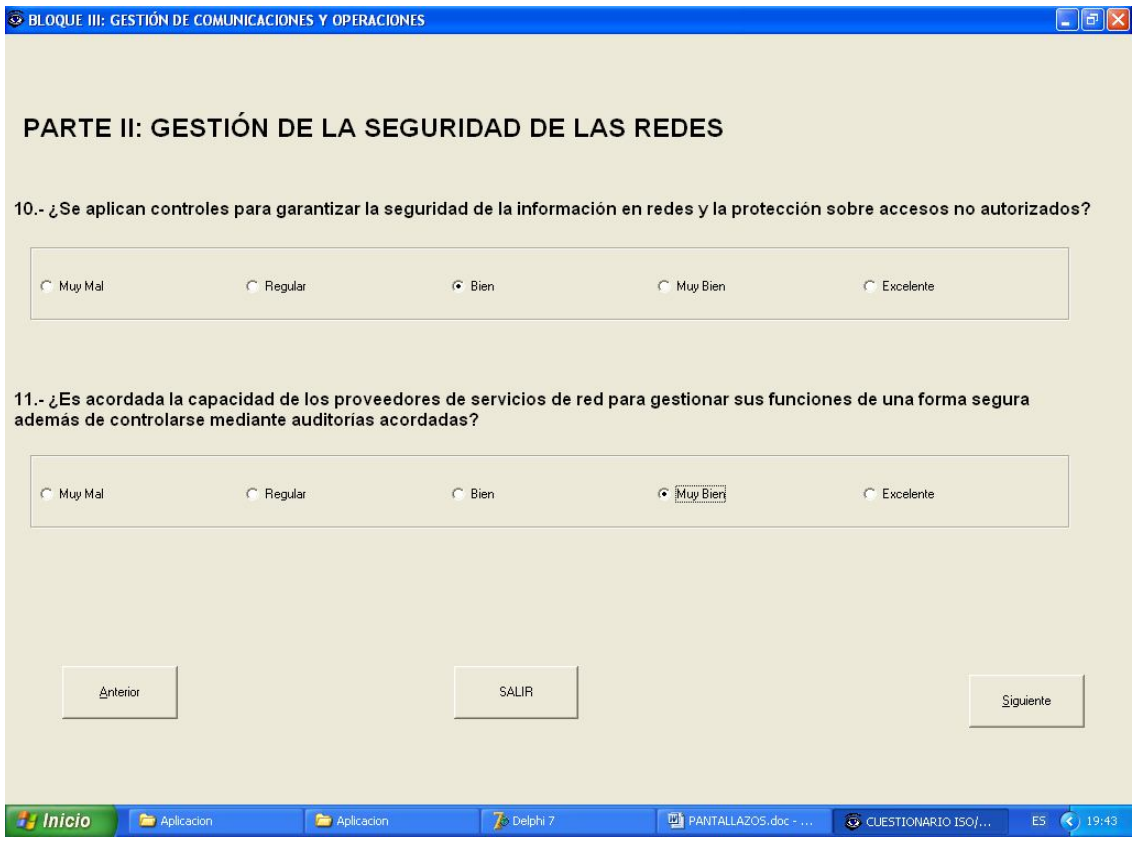

BLOQUE I: POLÍTICA DE SEGURIDAD
1.- ¿Existe un documento de política de seguridad de la organización donde consta: la definición de la seguridad de la empresa, la declaración de intenciones de objetivos, marco con los objetivos de control y explicación de términos generales sobre la política empresarial, así como las responsabilidades del personal y las referencias de la documentación aportada?
Muy Mal
Regular
Bien
Muy Bien
Excelente
2.- ¿Se revisan periódicamente las políticas de seguridad de la información para su actualización y mantenimiento?
Muy Mal
Regular
Bien
Muy Bien
Excelente
3.- ¿Todo el personal de la empresa tiene acceso y conoce las políticas expuestas en el documento?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:42


BLOQUE II: SEGURIDAD FÍSICA Y AMBIENTAL
BLOQUE II
SEGURIDAD FÍSICA Y AMBIENTAL
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:42


BLOQUE II: SEGURIDAD FÍSICA Y AMBIENTAL
4.- ¿Los equipos están protegidos sobre posibles amenazas físicas y ambientales?
Muy Mal
Regular
Bien
Muy Bien
Excelente
5.- ¿Existen unas instalaciones de suministro adecuadas ante posibles cortes de luz o pérdidas de información por posibles acontecimientos inesperados?
Muy Mal
Regular
Bien
Muy Bien
Excelente
6.- Está el cableado debidamente protegido, etiquetado y en instalaciones adecuadas?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:43

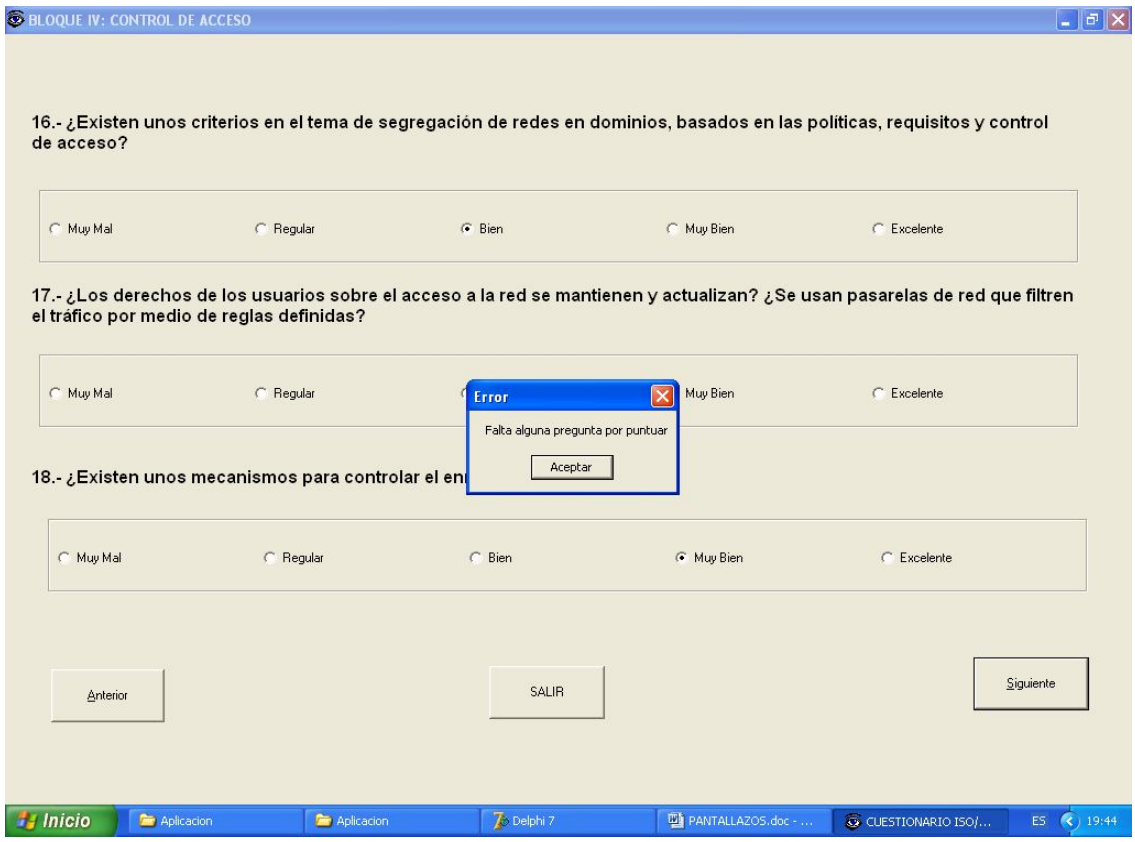

BLOQUE III: GESTIÓN DE COMUNICACIONES Y OPERACIONES
BLOQUE III
GESTIÓN DE COMUNICACIONES
Y
OPERACIONES
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:43


BLOQUE III: GESTIÓN DE COMUNICACIONES Y OPERACIONES
PARTE I: GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS
7.- ¿Los controles de seguridad, la definición de servicios y los niveles de prestación incluidos en el acuerdo de prestación de servicios por terceros son objeto de implantación y mantenimiento por el tercero?
Muy Mal
Regular
Bien
Muy Bien
Excelente
8.- ¿El seguimiento, y la revisión de los servicios gestionados por terceros garantizan que se cumple la seguridad de la información y los acuerdos del contrato?
Muy Mal
Regular
Bien
Muy Bien
Excelente
9.- ¿Se procura hacer mejoras continuas sobre las prestaciones de los servicios incluyendo el mantenimiento y mejoras de las politicas?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:43


BLOQUE III: GESTIÓN DE COMUNICACIONES Y OPERACIONES
PARTE II: GESTIÓN DE LA SEGURIDAD DE LAS REDES
10.- ¿Se aplican controles para garantizar la seguridad de la información en redes y la protección sobre accesos no autorizados?
Muy Mal
Regular
Bien
Muy Bien
Excelente
11.- ¿Es acordada la capacidad de los proveedores de servicios de red para gestionar sus funciones de una forma segura además de controlarse mediante auditorías acordadas?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:43

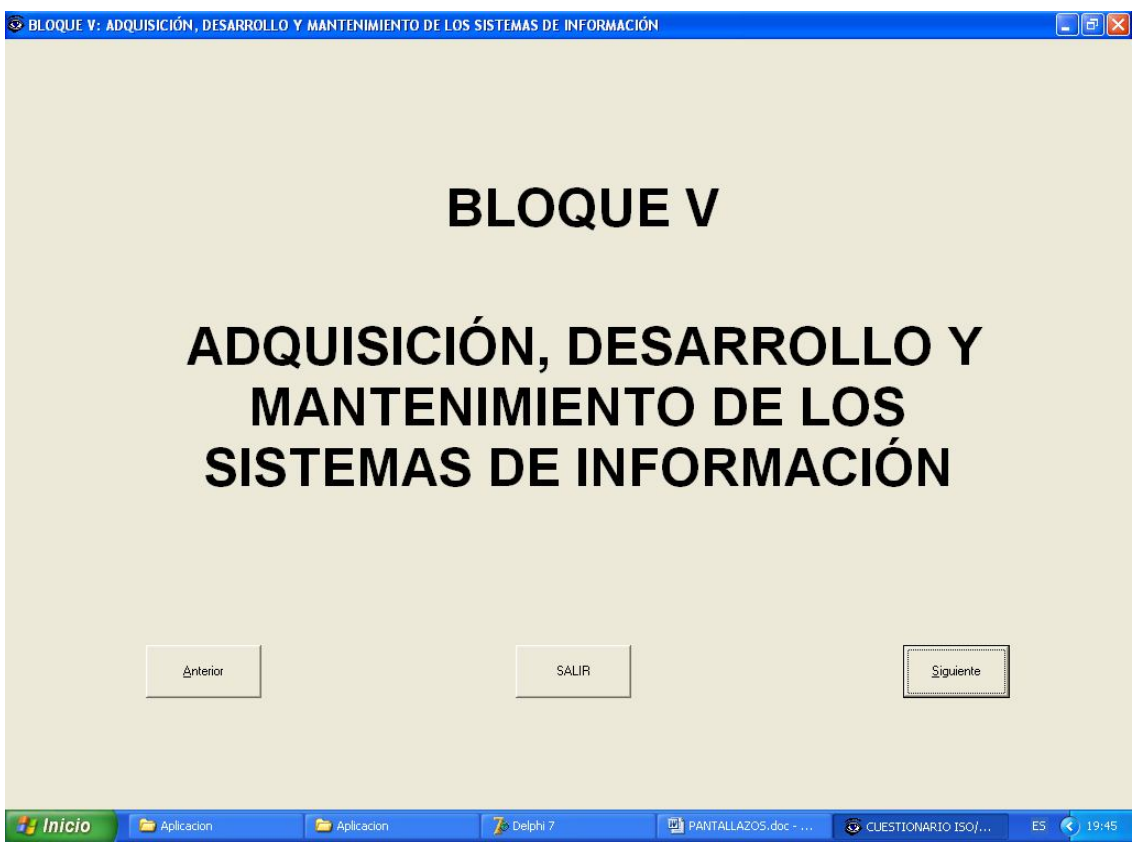

BLOQUE IV: CONTROL DE ACCESO
BLOQUE IV
CONTROL DE ACCESO
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:44

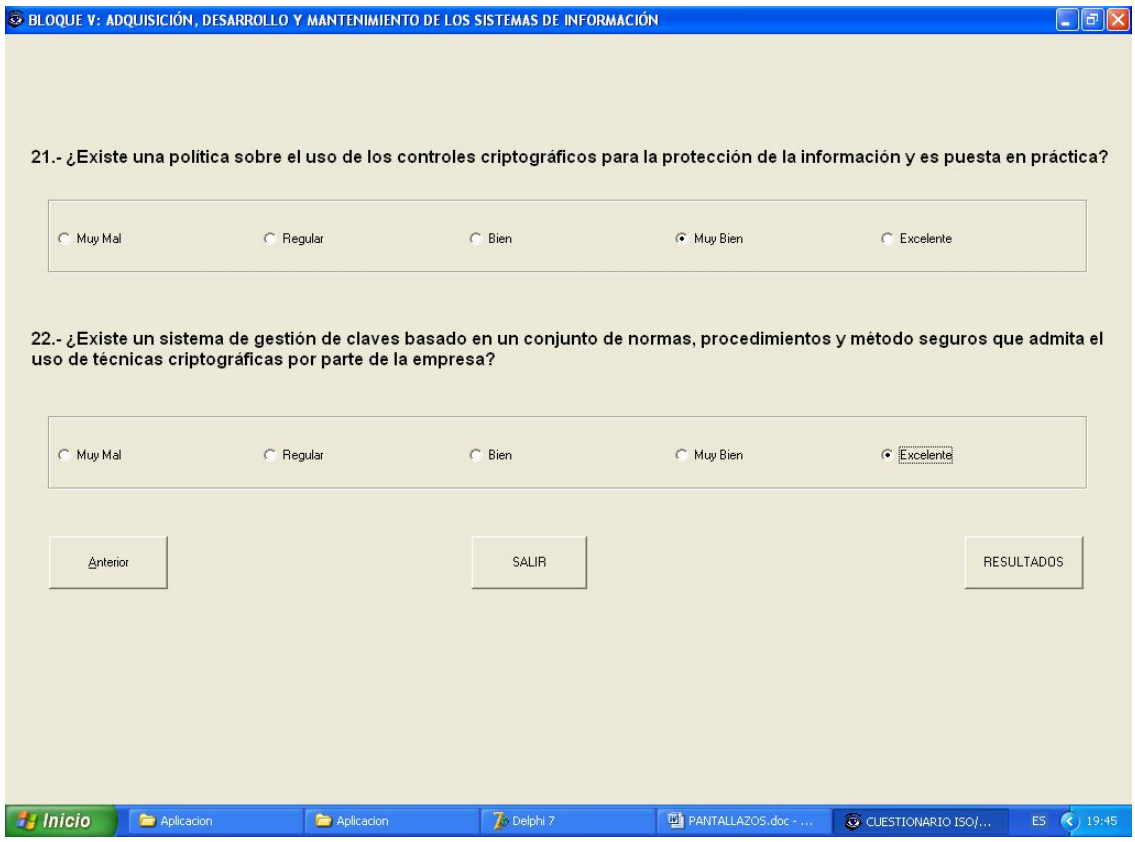

BLOQUE IV: CONTROL DE ACCESO
PARTE I: CONTROL DE ACCESO A LA RED
12.- ¿Existen unas políticas de seguridad sobre los servicios de red?, ¿Son llevadas a cabo?
Muy Mal
Regular
Bien
Muy Bien
Excelente
13.- ¿Están implantados unos métodos de autenticación lo suficientemente buenos que garantizan la seguridad de la información ante intentos de accesos no autorizados tanto en oficina como en remoto?
Muy Mal
Regular
Bien
Muy Bien
Excelente
14.- ¿Hay implantado algún método que controle por una parte al trabajador y por otra al equipo?, ¿Desde ciertos equipos sólo se puede acceder a aplicaciones concretas?
Muy Mal
Regular
Bien
Muy Bien
Excelente
15.- ¿Están debidamente protegidos los accesos a puertos que puedan ser conflictivos?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:44

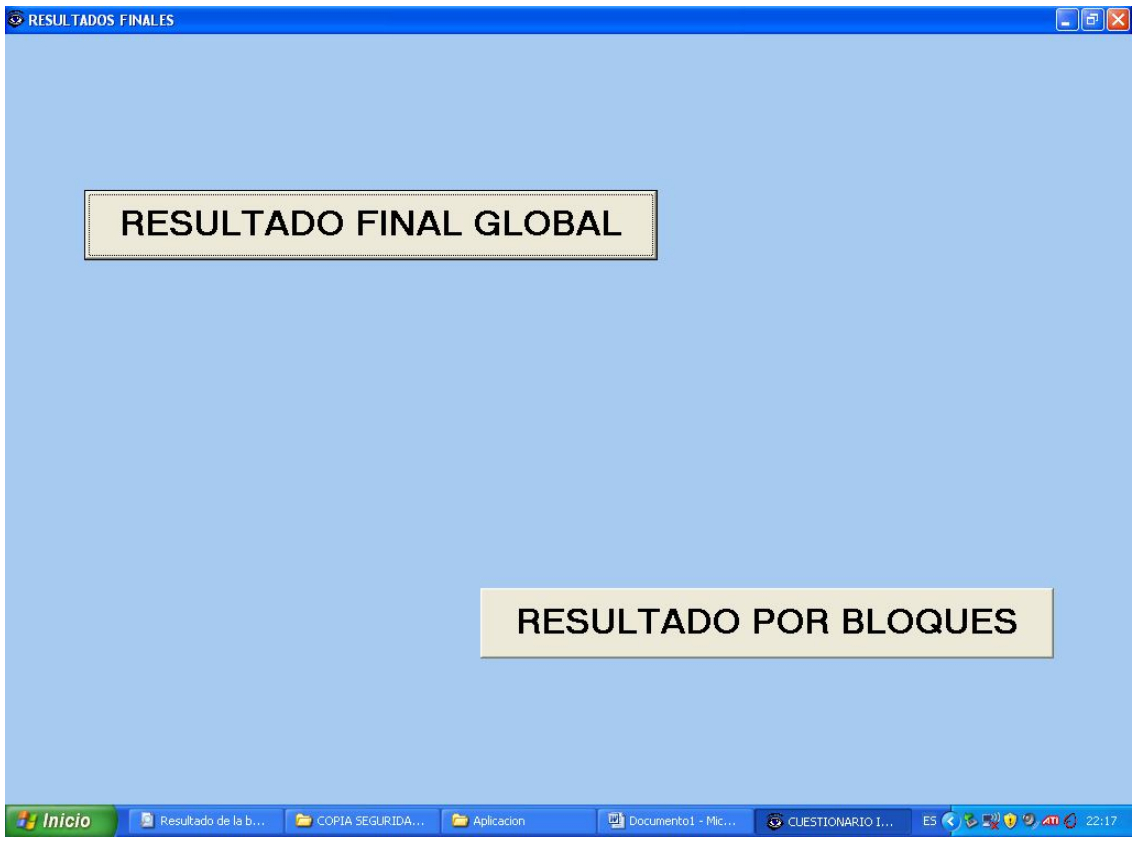


En la pantalla anterior se muestra el error que sale por pantalla si se deja alguna pregunta sin responder y se pretende pasar de pantalla.

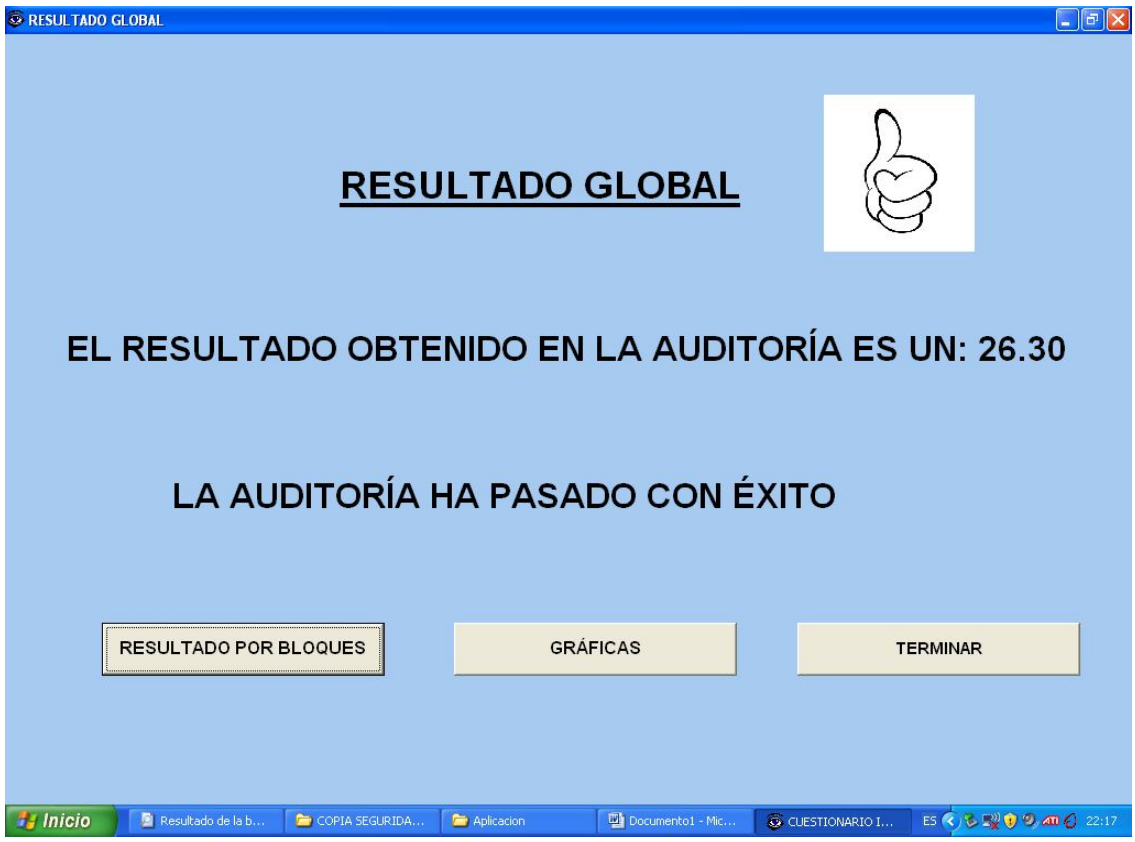

BLOQUE IV: CONTROL DE ACCESO
PARTE II: ORDENADORES PORTÁTILES Y TELETRABAJO
19.- ¿Se lleva un control sobre el uso de portátiles y dispositivos móviles?, ¿el uso de estos dispositivos de telecomunicaciones cumplen con las condiciones de seguridad establecidos en las políticas de empresa?
Muy Mal
Regular
Bien
Muy Bien
Excelente
20.- ¿En el tema de teletrabajo, dichas actividades son autorizadas y controladas por la gerencia y se garantiza que las disposiciones del lugar son adecuadas para trabajar?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:44


BLOQUE V: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
BLOQUE V
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
Anterior
SALIR
Siguiente
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:45


BLOQUE V: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
21.- ¿Existe una política sobre el uso de los controles criptográficos para la protección de la información y es puesta en práctica?
Muy Mal
Regular
Bien
Muy Bien
Excelente
22.- ¿Existe un sistema de gestión de claves basado en un conjunto de normas, procedimientos y método seguros que admita el uso de técnicas criptográficas por parte de la empresa?
Muy Mal
Regular
Bien
Muy Bien
Excelente
Anterior
SALIR
RESULTADOS
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:45

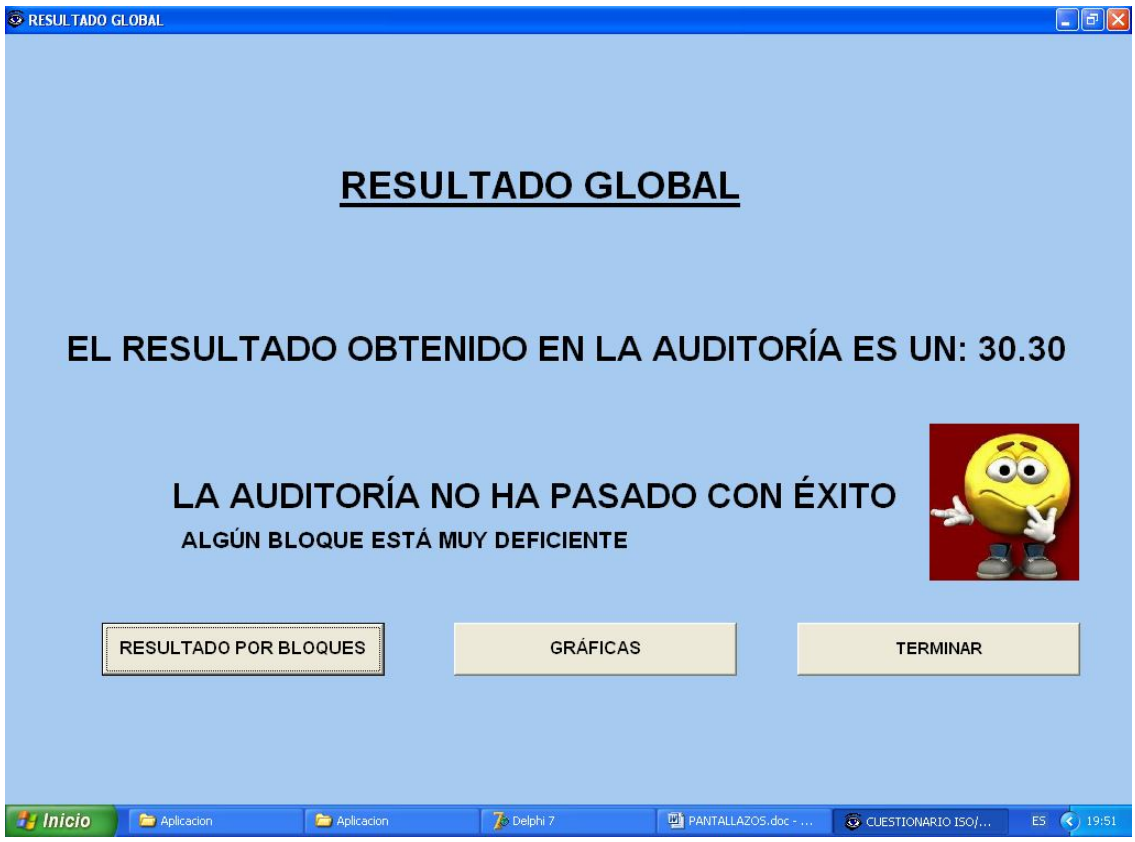


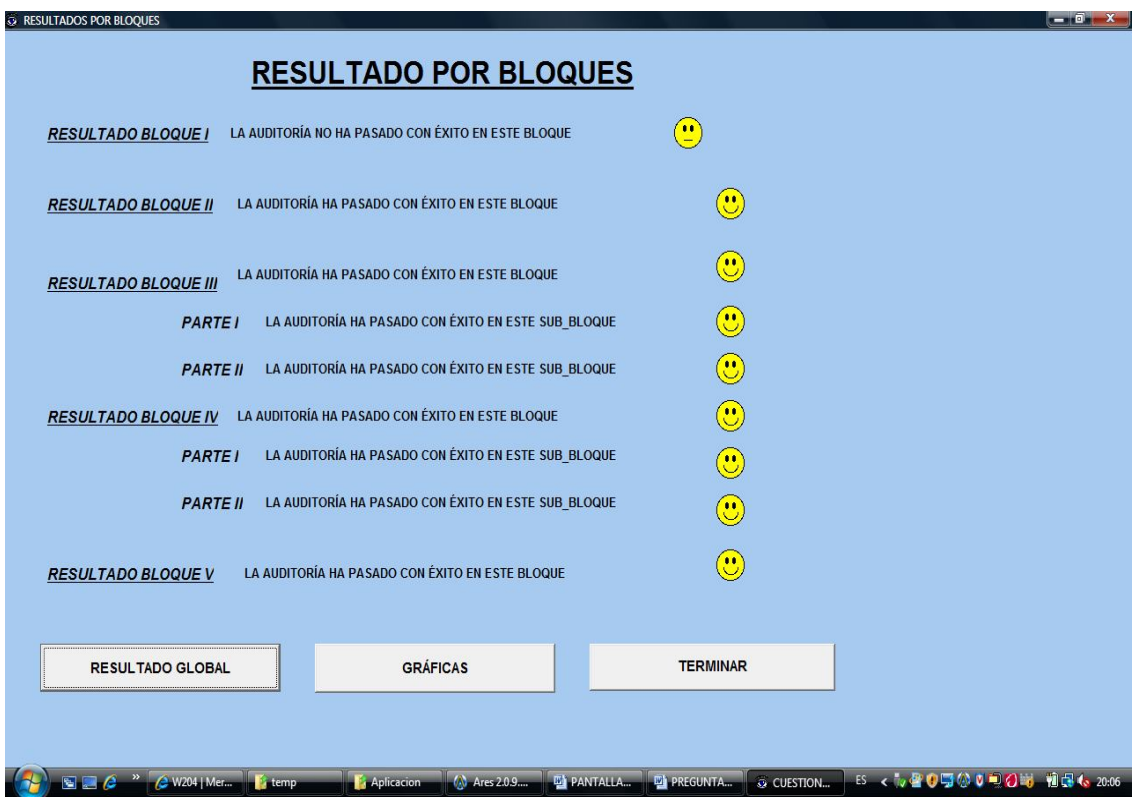
Ésta es la pantalla que aparece cuando se ha terminado el cuestionario. Da opción de ver el resultado final o de verlo por bloques y sub-bloques.



Ésta pantalla muestra el resultado global. En ella aparece un número que es el obtenido en la auditoría, éste cambia según los valores de los pesos que se introduzcan inicialmente. Por ejemplo con los valores por defecto se pasa la auditoría si se saca más de un veintitrés con setenta. En este caso se cumple la condición y por lo tanto la auditoría se pasa con éxito.

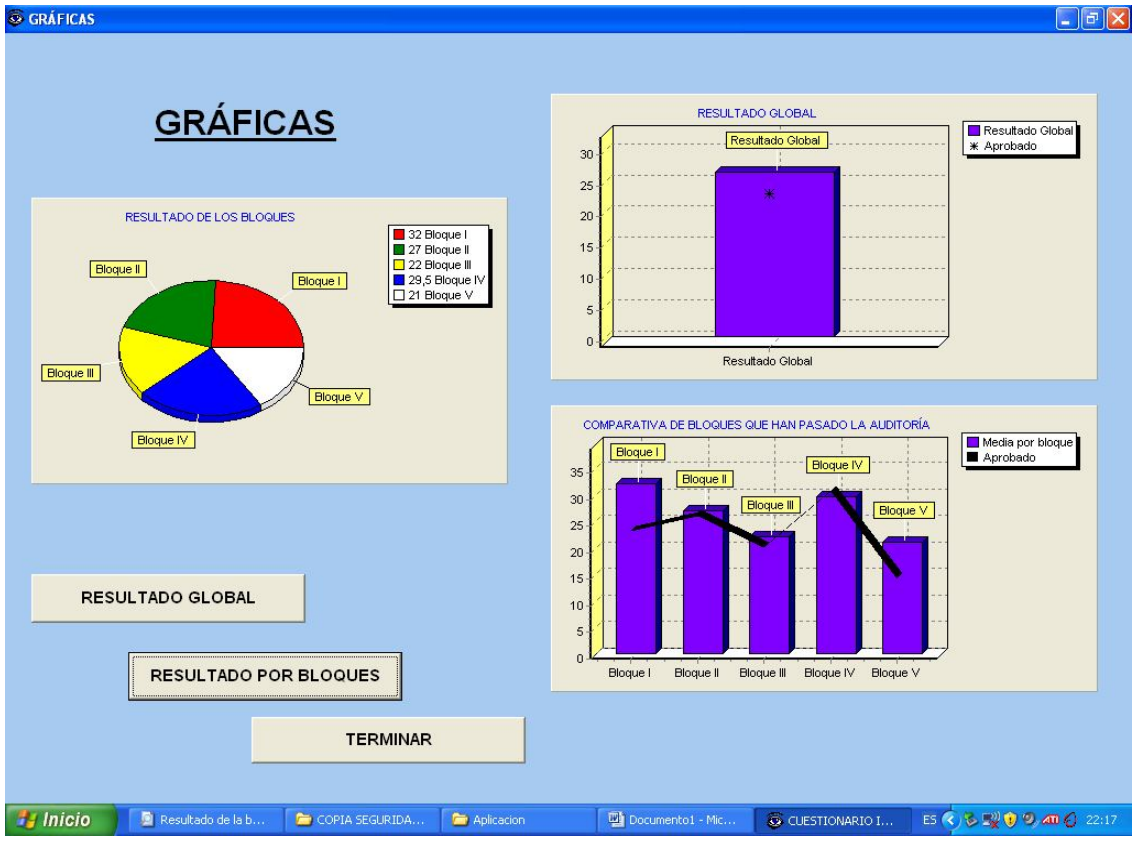
También puede darse el caso de que la auditoría esté en media aprobada pero alguno de los bloques esté especialmente mal, en este caso se mostrará un mensaje de que la auditoría no ha pasado con éxito indicando explícitamente que se debe a algún bloque que está especialmente defectuoso.


RESULTADO GLOBAL
RESULTADO GLOBAL
EL RESULTADO OBTENIDO EN LA AUDITORÍA ES UN: 30.30
LA AUDITORÍA NO HA PASADO CON ÉXITO
ALGÚN BLOQUE ESTÁ MUY DEFICIENTE
RESULTADO POR BLOQUES
GRÁFICAS
TERMINAR
Inicio
Aplicacion
Aplicacion
Delphi 7
PANTALLAZOS.doc - ...
CUESTIONARIO ISO/...
ES
19:51


RESULTADOS POR BLOQUES
RESULTADO POR BLOQUES
RESULTADO BLOQUE I LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO BLOQUE II LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO BLOQUE III LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE BLOQUE
PARTE I LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
PARTE II LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
RESULTADO BLOQUE IV LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE BLOQUE
PARTE I LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
PARTE II LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
RESULTADO BLOQUE V LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO GLOBAL
GRÁFICAS
TERMINAR
W204 | Mer...
temp
Aplicacion
Ares 2.0.9....
PANTALLA...
PREGUNTA...
CUESTION...
ES
20:06

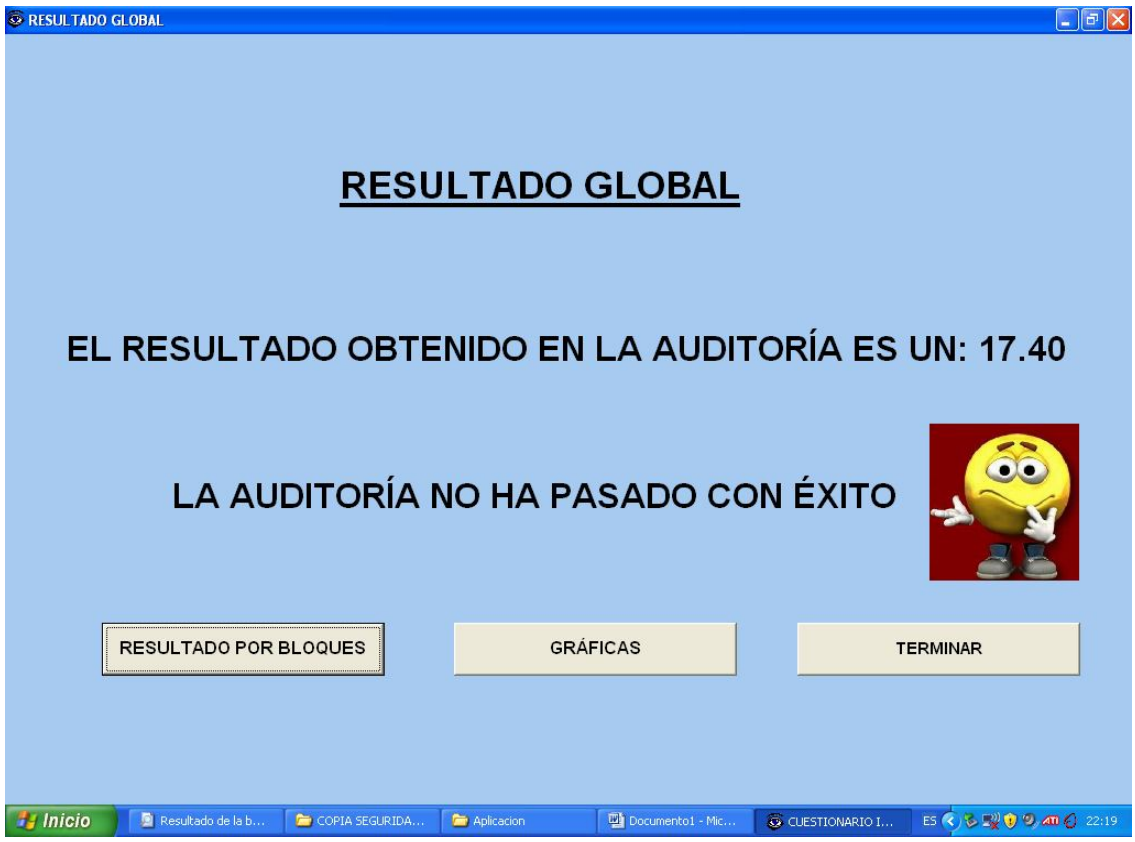
Así se ve el resultado por bloques.

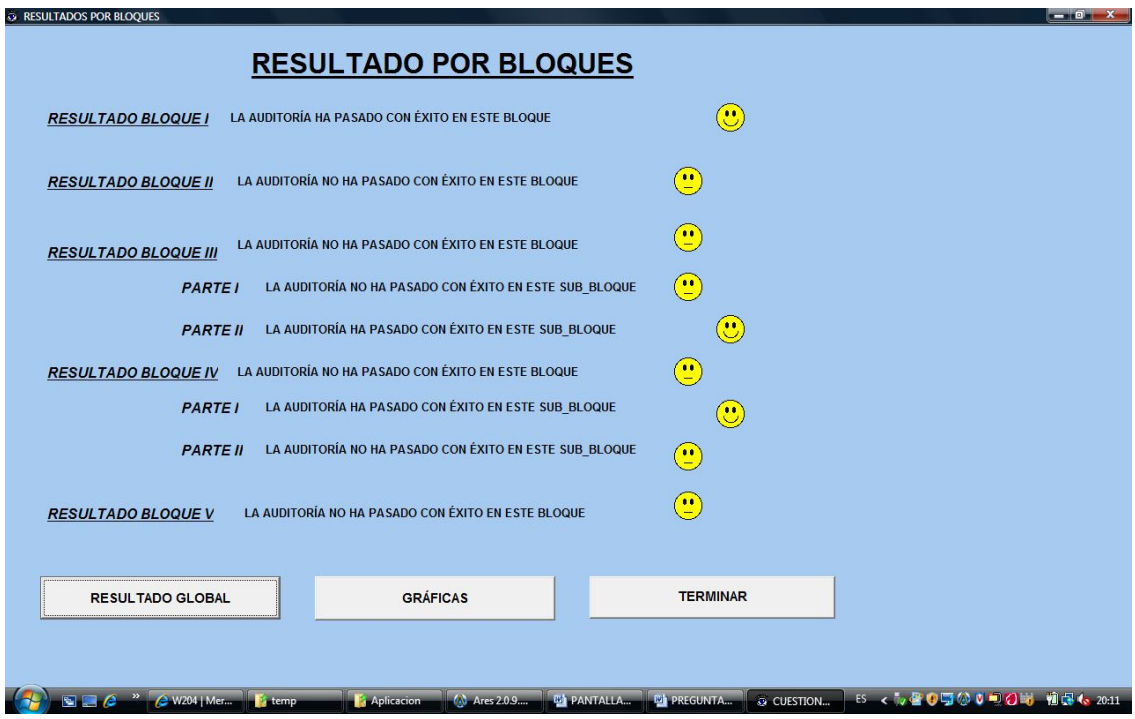
Si pinchamos en el botón de gráficas se muestra la siguiente pantalla:

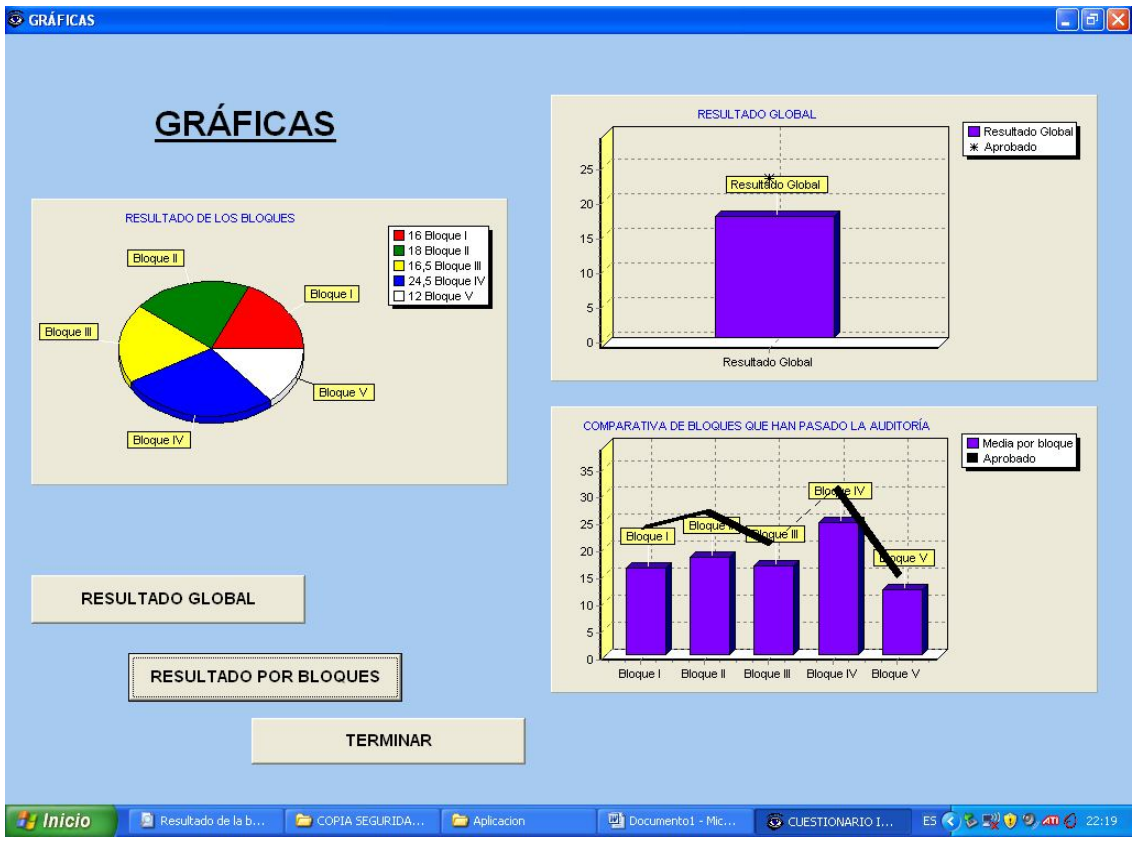


Finalmente cuando ya hemos visto todo podemos dar al botón de terminar y con ello se cierra la aplicación.

Ahora se muestran las pantallas de resultados en el caso de que la auditoría no pase con éxito debido a que la media obtenida en las preguntas es inferior a la que se necesita para pasar la auditoría.


RESULTADO GLOBAL
RESULTADO GLOBAL
EL RESULTADO OBTENIDO EN LA AUDITORÍA ES UN: 17.40
LA AUDITORÍA NO HA PASADO CON ÉXITO
RESULTADO POR BLOQUES
GRÁFICAS
TERMINAR
Inicio


RESULTADOS POR BLOQUES
RESULTADO POR BLOQUES
RESULTADO BLOQUE I LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO BLOQUE II LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO BLOQUE III LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE BLOQUE
PARTE I LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
PARTE II LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
RESULTADO BLOQUE IV LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE BLOQUE
PARTE I LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
PARTE II LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE SUB_BLOQUE
RESULTADO BLOQUE V LA AUDITORÍA NO HA PASADO CON ÉXITO EN ESTE BLOQUE
RESULTADO GLOBAL
GRÁFICAS
TERMINAR



El gráfico de sectores muestra los valores obtenido en los bloques, la gráfica de resultado global muestra el resultado obtenido y el asterisco muestra hasta donde le hacía falta llegar para aprobar.

Y la gráfica comparativa de bloques muestra también el resultado final obtenido en cada bloque y la línea negra indica hasta donde tenía que llegar cada bloque para pasar la auditoría.

Como se puede ver se siguen en estas pantallas los mismos criterios que si la auditoría pasara con éxito variando los datos como es lógico.

CAPÍTULO VI
ANEXOS

TÍTULO VIII DEL REGLAMENTO DE DESARROLLO DE LA LOPD

En el BOE del diecinueve de Enero de 2008 se hace referencia a el reglamento de desarrollo de la LOPD, puntos que nos interesan sobre ésta es el Título VIII que trata de las medidas de seguridad en el tratamiento de datos de carácter personal.

Este título está compuesto de cuatro capítulos:

- ***CAPÍTULO I :*** *Disposiciones generales*
- ***CAPÍTULO II :*** *Del documento de seguridad*
- ***CAPÍTULO III*** *: Medidas de seguridad aplicables a ficheros y tratamientos automatizados*
- ***CAPÍTULO IV*** *: Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados*

A lo largo de lo que se desarrolla en estos artículos se encuentran varios puntos relacionado con la ISO 27002 de la que se ha desarrollado la guía. Aparecen varios aspectos relacionados con el tratamiento de datos ya sea en control de accesos o en las políticas de empresa.
La primera parte hace más hincapié en la parte de tratamiento de información con ficheros.
La segunda se centra en el documento de seguridad que será aplicable a toda la empresa.
El siguiente punto se divide en dos partes, la primera habla de medidas de seguridad básica para el tratamiento de datos. Habla sobre el documento de seguridad y como éste debe ser comunicado a toda la empresa y algunos temas como la existencia de un registro de incidencias sobre problemas con los datos. También habla sobre temas de autenticación de usuarios y copias de seguridad de respaldo.

La segunda parte de este capítulo es sobre las medidas de seguridad medias, se divide en la parte del responsable de seguridad, habla de temas de auditoría, gestión de soportes y documentos, identificación y autenticación y de nuevo sobre el registro de incidencias.
La tercera sesión habla sobre las medidas altas de seguridad, trata sobre la gestión y distribución de soportes, copias de respaldo y recuperación y registro de accesos y finalmente tema de telecomunicaciones.
El capítulo IV también se divide en tres secciones sobre medidas de seguridad básicas, medias y altas. Sobre las básicas se centra en las obligaciones comunes, los criterios de archivo y los dispositivos de almacenamiento. Termina hablando de la custodia de los soportes.
Las medidas de seguridad media tratan los puntos del responsable de seguridad, y de nuevo temas de auditoría.
Las medidas de seguridad altas se centran en el almacenamiento de la información, las copias y reproducciones, el acceso a la documentación y el traslado de la misma.

A continuación se muestra la información recopilada.

TÍTULO VIII

CAPÍTULO I: Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cuál sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. Encargado del tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II: Del documento de seguridad

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el

encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III: Medidas de seguridad aplicables a ficheros y tratamientos automatizados

SECCIÓN 1. ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo

anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

SECCIÓN 2. ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título .Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN 3. ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV: Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

SECCIÓN 1. ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.

b) Niveles de seguridad.

c) Encargado del tratamiento.

d) Prestaciones de servicios sin acceso a datos personales.

e) Delegación de autorizaciones.

f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

g) Copias de trabajo de documentos.

h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.

b) Registro de incidencias.

c) Control de acceso.

d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del

fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

SECCIÓN 2. ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

SECCIÓN 3. ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

PUNTOS RELACIONADOS CON LA AUDITORÍA INFORMÁTICA

A continuación se muestra las fuentes originales de las que se ha sacado la información de algunos puntos del Capítulo III, Introducción a la Auditoría. Esta información se puede acceder a ella en la página de *www.isaca.org.*

P2 INTRODUCTION

1.1 The purpose of this procedure is to provide a tool to help evaluate a certification authority (CA), both in terms of quality of services offered and reliability.
1.2 The techniques of authentication play an essential role in electronic commerce, whether they are used to provide access to a corporate intranet, or to identify the communicating or transacting parties (private or commercial). Authentication of the parties to a transaction or communication is a method of building trust in electronic commerce, when appropriately carried out by reliable and secure technology infrastructures.
1.3 Authentication may be performed at various levels of security and by different technologies based on the party's requirements and the transaction or communication characteristics. For years, people have used passwords or similar methods of authentication, but today there are many more technological approaches to help facilitate this critical part of a communication. Today there are a variety of biometric and cryptographic key-based solutions used for authentication. They can be used as stand-alone systems, in combination or as part of a larger technological environment. Many organisations believe that public key infrastructure (PKI) based tools provide the most scalable solutions for commercially robust authentication systems.

2. TERMINOLOGY AND TECHNOLOGY NEUTRALITY

2.1 The term authentication refers to a large class of electronic applications whose functions may range from pure identification and authorisation to legal recognition.

2.2 Referring to specific authentication techniques, the terms electronic signature and digital signature are often used interchangeably. This has led to significant international confusion as to the use of the two terms. Digital signature is a functional subset of the more inclusive term electronic signature. Terminology used in this document shall refer to definitions with a certain level of international acceptance achieved through recognised international forums.

2.2.1 The term electronic signature has been defined by many authors as a signature in electronic form in, or attached to or logically associated with, a data message, and used by or on behalf of a person with the intent to identify that person and to indicate that person's approval of the contents of the data message.

2.2.2 Consequently, digital signature has been defined as a transformation of a message using an asymmetric cryptosystem such that a person having the signer's message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the signed message has been altered since the transformation was made.

2.3 The distinction between electronic and digital signatures has been at the core of international discussions on whether policies should focus on electronic signatures or digital signatures. The question is still open, and this procedure applies both to electronic signature and digital signature authentication techniques.

3. DIGITAL SIGNATURE AND KEY MANAGEMENT PROCEDURE

3.1 Verifying the security requirements for public-key security technology, involves a trusted third-party known as the certification authority (CA). The CA distributes the electronic keys used to encrypt and decrypt user and server information and the electronic certificates are used to authenticate users and servers.

General Aspect of a CA	Procedures and Perspectives	✓
Organisational management	**Suggested procedure(s):** Determine whether or not the CA has effective organisation structures able to facilitate the effective management of information and systems. **Perspective:** The organisational element must be carefully considered when reviewing a CA.	
Certification/ accreditation	**Suggested procedure(s):** Determine whether or not the CA has received accreditation by appropriate international standard organisations for secure communications. **Perspective:** The certifications and accreditations the CA has received from approved international standards organisations will provide valuable information related to the quality of their products and services.	
Technology architecture	**Suggested procedure(s):** Identify the appropriate and applicable standards (i.e., support for X.509 certificate and X.500 directory) and determine whether or not the technology architecture is based upon those. **Perspective:** The technology architecture should be based on standards to provide assurance, scalability and interoperability.	
Operations management	**Suggested procedure(s):** Identify what services the CA offers, such as registering users, issuing keys, updating keys, backing up and recovering keys, revoking and reissuing keys, disabling and reenabling keys. Determine whether or not the services administration and operation of CA, and external services and outsourcing are adequate. Provide reasonable assurance of the availability of a redundant/back-up site and professional support. **Perspective:** Adequate operations management will provide reasonable assurance the practices for supporting operations are effective.	

The purpose of the above controls is to understand how the CA operates and for data and document collection. Specific topics are covered by the following checklist:

P3. 1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The Management Guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The Management Guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 The purpose of this procedure is to provide the steps to be followed by IS auditors when reviewing an intrusion detection system (IDS).

1.3.2 This procedure is designed to provide the following:

- A definition of an IDS and how it functions
- The purpose and benefits of using an IDS
- The principal types of IDSs and the advantages and disadvantages of each
- Guidance on the conditions necessary to appropriately implement and administer an IDS
- Planning considerations when reviewing an IDS
- An overview of the audit approach
- Reporting issues
- Types of audit procedures and audit evidence

1.3.3 This procedure also defines IDS controls within the existing COBIT 3rd Edition, Framework, published in 2000 by the IT Governance Institute.

2. WHAT IS AN IDS?

2.1 Definition

2.1.1 Intrusion detection is the process of detecting unauthorised use of systems and networks through the use of specialised software and/or hardware. The primary purpose of an IDS is to provide the ability to view network and system activity in real time and to identify unauthorised activity. In addition, it can provide a nearly real-time automated response. IDS products also provide the ability to analyse today's activity in relation to past activity to identify larger trends and problems.

2.2 Purpose and Benefits of an IDS

2.2.1 The primary purpose of performing intrusion detection is to help prevent the consequences caused by undetected intrusions. Implementing a programme of effective security controls is an effective starting point for establishing the supporting security infrastructure. Effective controls grow out of effective information security policies, standards and practices and the use of appropriate technology. Appropriate technology is defined as technology that supports and enforces an organisation’s policy effectively.

Being able to detect an intrusion attempt in real time is an important aspect of intrusion detection. Knowing when an attack is in progress and being able to take immediate action significantly improves the odds of successfully terminating intrusions and tracing intrusion attempts to their source. Real-time detection depends upon having a watchdog system that sits in the background and monitors all activities involving the connected devices. The monitoring system must be able to interpret various incidents and diagnose actual attacks.

2.2.2 Most traditional IDSs take either a network- or a host-based approach toward identifying and protecting against attacks. In either case, IDSs look for attack signatures, specific patterns that ordinarily indicate malicious intent or suspicious activity. A truly effective IDS will employ both methods.

2.3 Principal Types of IDSs

2.3.1 The principal types of IDSs are:

- Host-based
- Network-based
  - Statistical anomaly
  - Pattern matching

2.4 Host-based IDS

2.4.1 Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit logs for suspicious activity. Because intrusions were rare, after-the-fact analysis proved adequate to prevent future attacks.

2.4.2 Host-based IDSs still use audit logs, but they are much more automated, having evolved to include more sophisticated and responsive detection techniques. Host-based IDSs typically monitor systems, events and security logs. When any of these files change, the IDS compares the new log with attack signatures to determine if there are any matches. If so, the system responds with administrator alerts and other calls to action. It monitors

files on systems for changes. The primary host-based IDS purpose is to monitor systems for individual file changes.

2.4.3. Host-based IDSs have expanded to include other technologies. One popular method of detecting intrusions checks key system files and executables via checksums at regular intervals looking for unexpected changes. The timeliness of response is directly related to the frequency of the polling interval. Finally, some products monitor port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

2.4.4 Host-based IDSs are not as fast as their network counterparts, however, they do offer advantages that network-based systems cannot match. These advantages include stronger forensics analysis, close focus on host-specific event data and lower entry-level costs.

2.4.5 The advantages of host-based IDSs include:

- They verify success or failure of an attack. While Network-based IDSs provide an early warning, host-based IDSs provide verification of whether an attack was successful or not.
- They monitor specific system activities. Host-based IDSs can monitor all user activity while connected to the network. It is very difficult for a network-based system to provide this level of event detail.
- They detect attacks that are not identified by network-based systems. For example, attacks from a keyboard inside a network may not be detected by a network-based system.
- They are well-suited for encrypted and switched environments. Since host-based systems reside on various hosts throughout an enterprise, they can overcome some of the problems of network-based systems in switched and encrypted environments. Identifying where to specifically place the IDS on internal networks can be difficult when trying to provide broad coverage for the enterprise. By the

time a host-based system reviews the traffic, the data stream has already been decrypted.

- They have nearly real-time detection and response. Many current host-based systems can receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response.
- They do not require additional hardware. Host-based IDSs reside on existing network infrastructure, including file servers, web servers and other shared resources.
- They have a lower cost of entry. Network-based IDSs can offer broad coverage with little effort and they are often expensive. Host-based intrusion detection systems are often priced in the hundreds of dollars for a single agent and can be deployed by with limited initial funding.

2.4.6 The disadvantages of host-based IDSs include:

- Their capabilities are compromised as soon as the host machine is compromised.
- They add additional overhead to an operating system and require a copy for every protected machine on a network.
- They are frequently compared to antivirus tools, so users tend to use just the antivirus, where the IDS provides security features not found in an antivirus software.
- They are very application-specific.
- They must be able to translate between Windows NT, UNIX, VMS and other mainframe operating system languages. There are very few IDSs today that provide that level of translation. Since portions of these systems reside on the host that is being attacked, host-based IDSs may be attacked and disabled by a clever attacker.
- They are not well-suited for detecting network scans of all hosts in a network since the IDS at each host only sees the network packets that it specifically receives.
- They often have difficulty detecting and operating during denial-of-service attacks.

- They use the computing resources of the hosts they are monitoring.

2.5 Network based IDSs

2.5.1 Network-based IDSs use raw network packets as the data source. Network-based IDSs typically utilise network adapters running in promiscuous mode to monitor and analyse network traffic in real time. Promiscuous mode makes it extremely difficult for an attacker to detect and locate. Attack recognition functionality uses two common techniques to recognise an attack signature:

- Statistical anomaly detection
- Pattern, expression or byte code matching

2.5.2 The advantages of network-based IDSs include:

- Their greatest asset is stealth.
- They can be deployed with no effect on existing systems or infrastructure.
- Most are operating system independent. Deployed network-based intrusion-detection sensors will listen for all attacks, regardless of the destination operating system type.

2.5.3 The disadvantages of network-based IDSs include:

- They are not very scaleable; they have struggled to maintain capacities of 100 Mbps.
- They are based on predefined attack signatures—signatures that will always be a step behind the latest underground exploits.
- IDS vendors have not caught up with all known attacks, and signature updates are not released nearly as frequently as antivirus updates.

2.6 Statistical Anomaly IDSs

2.6.1 In the anomaly detection model, the IDS detects intrusions by looking for activity that is different from a user's or system’s normal behaviour. Anomaly-based IDSs

establish baselines of normal behaviour by profiling particular users or network connections and then monitoring for activities that deviate from the baseline. **2.6.2** The advantages of statistical anomaly based IDSs include:

- Many security experts feel they are capable of detecting never-before-seen attacks, unlike pattern matching-based IDSs that rely on attack signature analysis of past attacks.
- They can detect unusual behaviour and thus have the capability to detect attacks without having to be specifically programmed to detect them.

2.6.3 The disadvantages of statistical anomaly-based IDSs include:

- Often produce a large number of false positives due to the unpredictable nature of users and networks.
- Anomaly-based detection approaches often require extensive training sets of system event records to characterise normal behaviour patterns.
- Careful hackers can evade or disable them.

2.7 Pattern-matching IDSs

2.7.1 The majority of commercial products are based upon examining traffic, looking for documented patterns of attack. This means that the IDS is programmed to identify each known exploit technique. This can be as simple as a pattern match. The classic example is to examine every packet on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server. Some IDSs are built from large databases that contain thousands of such patterns. The IDS monitors every packet, looking for packets that contain one of these defined patterns.

2.7.2 The advantages of pattern matching IDSs include:

- They have a shorter implementation timeline than anomaly IDSs. However, there must be a pattern-matching engine running on the network that looks for events that fit the specific pattern definitions.
- They are easy to implement, deploy, update and understand.

- They produce fewer false positives as compared to anomaly IDS because they produce higher numbers of false negatives. In other words, it is easier to slip something past a pattern matching detection system, but they are fast.

2.7.3 The disadvantages of pattern matching IDSs include:

- Normal network traffic causes many false positives, but less relative to anomaly-based IDS.
- Careful hackers can evade or disable the IDS.
- They cannot detect anything for which they do not have a pattern.
- They require constant updating with new rules.
- They are easier, as compared to anomaly-based IDSs, to fool by sending fragmented packets across the network.
- The majority of pattern updates are provided by the vendor of the IDS, giving a role in network security to the vendor. The ability of the vendor to provide patterns for newly discovered attacks is a key in maintaining an effective pattern-matching IDS.

3. PROCEDURES TO REVIEW IDS IMPLEMENTATION

	Suggested Procedures	
Planning the review	An integral part of planning is understanding the organisation's information system environment to a sufficient extent for the IS auditor to determine the size and complexity of the systems and the extent of the organisation's dependence on information systems. The IS auditor should gain an understanding of the organisation's mission and business objectives, the level and manner in which information technology and information systems are used to support the organisation, and the risks and exposures associated with the organisation's objectives and its information systems. Also, an understanding of the organisational structure	

	including roles and responsibilities of key IT staff responsible for maintaining the IDS should be obtained.	
	Develop objectives to address the seven COBIT information criteria and have the organisation agree to them. The seven COBIT information criteria are: • Effectiveness • Efficiency • Confidentiality • Integrity • Availability • Compliance • Reliability of information	
Positioning of an IDS within the network architecture	Determine where the critical assets are placed throughout the network and at what point an organisation wants the detection to begin. For example, if an organisation wants to review the traffic outside its perimeter router, a sensor should be placed in front of the perimeter router. If there are concerns with traffic entering the network beyond the perimeter router and firewall and before critical servers, then sensors should be deployed at that point. Factors that must be taken into account when determining where to place an IDS include: • Is it desirable to have network traffic monitoring beginning inside or outside the network architecture? • Placing sensors on certain high-volume segments of a network could result in network latency. There could be a trade off between protection and production. • Multiple sensors may be required to monitor for different	

	vulnerabilities and to help support load balancing. This provides reasonable assurance that packets being passed will be thoroughly inspected, enhancing intrusion detection capabilities. This concept is referred to as “defence in depth.” • What servers/applications are at risk and what effect a denial-of-service (DOS) attack would have on the organisation? Sensors should be placed in these areas.	
Installation parameters	Determine whether the: • System is configured either to push data to or pull data from the analysis engine. Pushing data is the preferred method. Push can be configured to report attacks to the analysis engine as they occur. A disadvantage of the push method is that the sensor sends responses to attackers, which can aid attackers with identifying the sensor and launching additional attacks against the sensor. To mitigate this weakness, sensors can be configured to send data to the analysis engine even if an attack does not occur. For the pull method, the analysis engine obtains data from the sensors and waits to be queried. It is still capable of sending alerts in this mode, but queries need to be made to get details. • IDS is configured to recognise patterns and user behaviour. An IDS should be configured to differentiate between normal and abnormal network traffic. This also includes configuring the system to recognise/identify well known malicious signatures (i.e., worms, Trojans). For example, if the IDS identifies someone from outside the network with	

	the same address space as someone inside the network, this should raise a red flag that someone is spoofing the network. • IDS provides a feature for remote management.	
	Evaluate IDS configuration parameters to scan for attacks. Certain parameters can crash a system or application, rendering a system unusable.	
	Provide reasonable assurance that: • The IDS is configured to identify suspicious files and database modifications or even unexplained files that have been added. • User accounts, system files and log files are monitored for tampering. • The IDS is configured to send alerts when high-level intrusions occur and to minimise alerting resulting from false positives and low level attacks • The IDS operates based on attack signatures (misuse detection). • Alerts either by page, e-mail or other means can be sent. • A reporting module exists to aggregate attacks over a given period (i.e., hourly, weekly, monthly). • Filters are positioned based upon security policy to minimise false positives.	
Relationship to firewalls	Determine that the IDS does not require software to be installed on the firewall.	
	Provide reasonable assurance that appropriate actions are taken	

	when intrusion incidents are identified. Incident response procedures should be developed in conjunction with IDS implementation. The basic approach to responding to network attacks should include preparation, detection, containment, eradication, recovery and follow-up.	
	Suggested Procedures	
Other important control issues	Determine whether: • Any employees connect to the network through unauthorised modem lines (referred to as rogue modems) • Any employees run unauthorised software posing a security threat, such as any remote control software, e.g., Back Orifice • Certain e-mail attachments containing malicious code are restricted, without hampering productivity • Personnel is abreast of URLs that may pose a security threat, as some web sites are configured to exploit a network as it browses these sites • Correct action is taken on incidents noted from IDS. For example, determine that disciplinary action is taken if employees are found snooping around the network and running hacker tools.	
	Document the system flow process by gathering information including both the computerised and manual aspects of the system. The focus should be on the processing related to data flows that are of significance to the audit objective. The IS auditor may find, depending upon the processes and the use of technology, that documenting the transaction flow may not be practical. In that event, the IS auditor should prepare a high level diagram or narrative and/or utilise quality system documentation if provided.	

	Identify and test the IDS controls. Identify specific controls to mitigate risks and obtain sufficient audit evidence to determine that the controls are operating as intended. This can be accomplished through procedures such as: • Inquiry and observation • Review of documentation • Testing of IDS controls	
	Determine whether: • A third party provides information and assists in incident response • The system communicates with firewalls/routers and that this communication is secured, or is a separate channel/network required for secure communications (a parallel control network) • The IDS includes a tool for generating written reports that summarise the daily event log • Automated response mechanisms are available	
	Provide reasonable assurance that: • Signatures are updated often. • Updates are distributed via a secure method (such as encrypted or digitally sealed). • The IDS can detect many different types of attacks. • The false-positives are managed based on the level of risk. • The IDS requires updates to its rules. • A specialised figure is in place for providing/updating IDS rules. • Information about the latest attacks is used to keep the IDS	

	updated. • The IDS is effectively scalable (such as many sensors can be monitored/managed at a time). • The product has a low effect on network/host performance. • Other performance issues the IDS raises can be controlled. • The maximum bandwidth the system has been measured to analyse without loss, so that it provides 100 percent analysis coverage, is compatible with organisation needs. • The IDS analyses all network protocols in place if the organisation is network-based. • The IDS has the capability to analyse the upper level application protocols with sufficient detail. • The IDS does not require software to be installed on the host. • The communications between the sensor and the central manager are robust enough. • Alarm capture is reliable. If a high volume of alarms is generated, all of them are to be captured and put into a database. • Data obtained from the IDS are appropriately and effectively managed (i.e., data visualisation is a key issue). • A detailed procedure is in place explaining the actions to be taken when the IDS detects a problem. • The operating mechanism of the IDS is known by personnel. • The IDS can be used to accomplish other adjunct network management activity such as network device management. • The IDS is appropriate for deployment on the perimeter of the network as well as inside the network. • Product detects internally-generated abuse by authorised users over a long period of time. • The IDS is customised or configured to meet specific site policies and requirements.

	• List of people having access to the IDS is small and controlled. • Expertise and training are conducted to set up and maintain the IDS and analyse the results on a regular basis. • The IDS takes advantage of logs produced by other systems. • The IDS integrates with other vulnerability assessment products. • The IDS can respond reactively (communicate with firewalls/routers to block packets from a presumed attacker's IP net address). • The IDS reporting tools are efficient and accurate (lists of events, GUIs with icons representing events). • The methods for alerting the IDS operator/security manager are efficient and effective.
Reporting	Report weakness to management. Weaknesses identified in the IDS review either due to an absence of controls or to noncompliance should be brought to the attention of management. Where weaknesses identified during the intrusion detection system review are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.
	Consider including in the report recommendations to strengthen controls.

P4

1. BACKGROUND

1.1 Introduction

1.1.1 An antivirus and malicious logic policy should form part of the global security policy of the organisation. It also should provide the framework for procedures on prevention, detection and correction of viruses.

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."
1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processe, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT

applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.
1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

2. PREVENTION, DETECTION AND CORRECTION OF VIRUSES AND OTHER MALICIOUIS LOGIC

2.1 The IS auditor should provide reasonable assurance that the organisation has effective documented procedures on the prevention, detection and correction of viruses. The checklist below should be used as a guide by the IS auditor.

Suggested Procedures for Preventing and Managing Virus Infection	
Review management's analysis and assessment of critical resources and the types of protection to implement. The organisation antivirus policy should be based on an assessment of risk and vulnerabilities to best protect the organisation's information systems.	
Through discussions with IT, identify all possible types of inputs into computer systems, such as: • Physical media—diskettes, CD-ROMs and, more generally, any removable media • Peripherals to PCs—modems, devices connected via serial, USB or infrared ports (including PDAs or cell phones) • Remote connections from laptops operating outside the organisation • Network connections with identified third-party organisations such as customers, suppliers and administrations • The Internet protocols allowed by the organisation (HTTP, FTP and SMTP)Special attention should be paid to modems since users can use dial-up connections without the organisation being aware of it. For example, laptops,	

which are often enabled to access LANs and the Internet through an internal or external modem, might be vehicles for virus infection. Additionally, these modems can be used to allow users to access organisation assets in an uncontrolled manner. External vendors pose a serious threat if the policies at the third-party organisations are weak or nonexistent.	
Identify risks considering potential weaknesses of all layers of software installed on each platform, such as, operating systems, services (such as TCP/IP stack, mail checker), mail, web browser and other application software. Many types of code can be executed and trigger viruses (such as, when a service is started or activated).	
Based on the organisation's assessment of risk of virus exposure—often made as part of the organisation's overall risk analysis—examine selected hardware components and their related systems to determine which types of files and resources are allowed to run on the system, such as: • Harmful code loaded at system start-up on a bootable device • Executable file launched by the operating system • Code interpreted or run together with an application (such as DLLs, Java, Vba) • Script or macro A risk assessment should have been performed to determine what files and resources should be available for each system. The IS auditor should compare existing files and resources to the related hardware/software standard. The IS auditor should also review the standard against current best practices to identify whether any potential weaknesses may exist.	
Review the antivirus policy for end users, because different types of users may have different behaviours and different resources and methods available to perpetuate the virus. Viruses may be introduced by different categories of users: • The organisation's employees	

• Other staff working in the organisation (such as, consultants, contractors, temps) • People from outside of the organisation, including customers, vendors and other third parties The results of this analysis will be helpful in reviewing the organisation's policy to determine if it is appropriate and addresses all risks associated with the users of the organisation's systems.	
Review the network architecture of the organisation to determine the paths viruses can use to spread: • LANs are the most common ways for virus to propagate within the organisation. • Servers may store and spread viruses, such as, through a mailing application. • E-mail, web mail, downloads, unpatched operating systems, employees or contractors bringing in infected diskettes • Use of e-mail/firewall technology to block specific file types or attachments known to contain malicious code This evaluation will help in reviewing the antivirus architecture to identify key points where viruses can be scanned. A program should be in place to communicate the policy to end users and to build end-user awareness.	
Review the antivirus policy measures aimed at avoiding virus infection. This consists mainly of organisational procedures and communication within the organisation.	
Review rewrite access and execution rights, as well as the operating system and key application configuration on users' workstations. The policy should mention how users may enter data into the system or run code on their machines. For example, depending on the user's needs: • Removable media may be disabled • Downloading some types of files from the Internet may be forbidden, either	

via e-mail or the web (for example, executables or Visual Basic files may be filtered) • Macros can be disabled or macros-free types of documents preferred (such as, RTF, CSV) • Viewers can be used instead of complete applications, if modification is not needed • Automatic e-mail virus detection and eradication In any case, write access and execution rights should be carefully set up and reviewed, as well as the operating system's configuration on users' workstations.	
Review organisation policies on unauthorised software to determine what restrictions exist on the use of unauthorised software and how those restrictions are enforced. While ideally users will not have the right to install software by themselves on their workstations, in most instances, this capability exists. As a result, the organisation should have methods to detect and assess the risk of unauthorised software being installed by employees.	
Assess the risk of staff members introducing malicious code for internally developed software. This may also be achieved by referring to existing procedures, including user acceptance testing on separate equipment before implementing in production.	
Review vendor information resources for security bug fixes. Procedures should ensure these patches are installed in a timely manner.	
Determine the backup strategy of the organisation. Since restoration of systems, application and/or data may be necessary due to a virus occurrence, the person in charge of the policy should ensure this strategy is sufficient to restart equipment without major losses of data after a virus outbreak. As most viruses cause a loss of data at the workstation level, it is important that users are made aware of policies and procedures surrounding the backup of data on workstations.	
Review policies to mitigate the risk of virus infection, i.e., preventive actions to avoid infection:	

• The types of documents or files that may prove harmful • The risks associated with e-mails • Reporting suspect behaviour of the systems in use Users take an important part of the prevention effort against viruses. One of their roles is to identify potential sources of infection.	
Review the organisation's assessment and mitigation of its risks if it propagates viruses to others. Clauses limiting an organisation's responsibility should be added at the end of outgoing e-mails and to the various contracts and agreements with entities with which the organisation shares data.	
Determine whether the antivirus software policy is clearly defined and applied. Although prevention is an important part of an antivirus policy, it is essential to be able to detect viruses efficiently as soon as they get into the systems.	
Evaluate antivirus software for the four levels where viruses may be checked: • User workstation resources, such as floppies, hard disk drives and removable media • File servers—incoming and outgoing files • Mail applications—attached files, which may include executable code • Internet gateways—incoming flow of data (SMTP, HTTP, FTP protocols) and active components (such as Java and ActiveX) The policy should describe which antivirus software is to be installed at each point identified during the threat analysis. For example, a computer accessing the Internet via an ISP should be protected locally to detect viruses before they spread.	
Perform standard technical analysis of the antivirus suppliers, and evaluate their malicious code procedures. Some issues to consider are: • How often definition updates are published • How fast special updates are delivered when a major outbreak occurs • By which means and how quickly the vendor communicates new threats	

• What administration tools are provided to help with deployment and updating • What assistance the vendor offers in case of an outbreak Depending on the threat analysis results and the complexity of the organisation, antivirus software from several vendors can be chosen. For example, installing one antivirus application on user workstations and another on mail servers may maximise the chances of detecting viruses, especially if these antiviruses use different technologies. Additionally, the organisation must manage the increased complexity of getting updates from multiple antivirus vendors.	
Determine whether the organisation has assessed the use of full scan technology versus the corresponding loss of performance. Verify if the organisation has performed such analysis and appropriately considered its result (if the loss of performance in doing a full scan is unacceptable, users tend to disable or circumvent the antivirus software in their systems, resulting in an increased exposure). The policy defines which type of scanning is to be applied depending on the resource considered and the threat evaluation. It should state how often or in which conditions on-demand checks should be triggered, as on-access scans are CPU-consuming. For example, the types of files to examine must be listed. Two types of scanning are ordinarily provided by antivirus software: • On-access, the antivirus monitors all data accessed in real time without any user intervention and should run permanently at least on file servers, mail servers and Internet resources • On-demand, the antivirus software must be launched to check a specific resource at a given time • Other scanning procedures should also be considered. For example, some organisations have one server that scans many others instead of loading virus protection software on multiple machines. This type of scan works in conjunction with “active” scanning.	
Review the organisation’s procedures for the reporting of virus occurrences. This	

should include to whom in the organisation virus identification is reported (such as, help desk, antivirus taskforce), incident response procedures and event reporting. The occurrence of a virus within the organisation should be reported immediately and the organisation should have appropriate response procedures in place. These should include specifications as to what procedures should be followed, limits on who can disable or alter the configuration of antivirus software installed on user workstations, escalation and reporting procedures.	
Provide reasonable assurance that the frequency and scope of antivirus software updates are according to the recommendations of the antivirus software editor, organisation policy and the risk associated with each IT environment. Two types of updates are ordinarily available: • Engine updates, where the core of the antivirus software is changed • Virus definition updates, which are published when new viruses are discovered	
Provide reasonable assurance that virus definitions and antivirus engine updates, like any other software update, are tested on separate equipment before being implemented in a production environment. Some editors also publish emergency definition updates when a major outbreak occurs; a procedure must be set so management is immediately aware of these updates and can rapidly apply them (after appropriate testing is performed). Many antivirus software products come with automatic update features for both workstations and servers. This functionality should be taken into consideration, as manually performing updates can be a labour-intensive effort on large networked systems with multiple servers and workstations.	
Provide reasonable assurance that the status of the antivirus update is appropriately monitored by IT staff for completeness and accuracy: a single workstation not updated can constitute the starting point for a virus outbreak. In a LAN environment, the antivirus updates are always installed on servers by IT staff. Conversely, installation on clients/workstations is often delegated to users.	

Provide reasonable assurance that a policy exists to cover the use of tools, such as firewalls, in the antivirus strategy. Tools are not dedicated to dealing with viruses, but may help detect Trojan horses when they are activated. Other software products can detect suspect behaviour of mailing applications.	
Review existing procedures designed to halt the outbreak of a virus and to correct infected resources in case a virus is not detected and eradicated by the antivirus software (i.e., it may be necessary to shut down servers and/or disconnect physical connections to the network). These procedures should be triggered whenever a virus infection is suspected. The policy should detail the measures taken to stop the outbreak. Depending on the type of virus, some applications may have to be halted temporarily, such as, a mail application or a file server. Part of the organisation's network can also be isolated, if needed. The virus may either have entered the system because it bypassed detection paths or because its definition is not listed yet in the antivirus software databases. Therefore, the policy must specify the execution of on-demand checks after updating virus definitions. In case no virus can be located, the antivirus vendors can be sent suspected files for inspection.	
Provide reasonable assurance that a damage assessment is conducted to determine which parts of the systems were affected by an outbreak. Backups may be used to recover environments, programs and/or data. After checking that the antivirus software has been updated to deal with the new virus, the system can be restarted. Provide reasonable assurance that backup and restoration files are not infected with virus.	
Review the organisation's notification and alert process to assess whether other entities within the organisation are made aware of any outbreak, since they may have been infected as well. The policy should describe the way to deliver this information to the appropriate partners in a timely manner.	
Provide reasonable assurance that the antivirus policy is thoroughly documented, and procedures written to implement it at a more detailed level. Any procedure without proper documentation, is ineffective	
Provide reasonable assurance that policies and procedures are in effect for	

appropriate custody and retention of the documentation that support the formalised antivirus policy. Documentation should be retained to ensure proper follow-up.	
Provide reasonable assurance that users are trained in the procedures for an antivirus security policy, including testing of material learned. After successful testing has been completed, users should sign a document that describes their role within the policy. Users are to be informed about the antivirus security policy by such means as: • Employee meeting presentations • E-mail notifications • A security awareness web site	
Conduct an assessments on how the procedure is applied and its effectiveness on a recurring basis for each of the following areas: • Policy documentation • Threat analysis • Prevention of infections • Infection detection tools • Infection correction The results of policy assessments and the evolution of the organisation should be reviewed regularly and used to update the antivirus policy.	

TECHNIQUES TO ASSESS EFFECTIVENESS OF THE VIRUS AND OTHER MALICIOUS LOGIC POLICIES AND PROCEDURES

Suggested Techniques to Assess the Effectiveness of the Virus and Other Malicious Logic Polices and Procedures	
Evaluate use of proactive measures, including the maintenance of operating systems	

with all current patches and fixes; content filtering at gateways; enterprise-wide security awareness program, including reminders or follow-up programs; attachment stripping (such as .exe, .com, .vbs); use of “sandbox” methodology; restrict access to web-based e-mail sites at firewall or desktop level; and, block downloads from Internet, except for those that justify need.	
Obtain an understanding of the current network infrastructure (network architecture and design) by using network diagrams that document it.	
Determine if all types of desktops/PC, laptops, PDAs, file servers, e-mail gateways, Internet connection points, major types of software, remote locations, WAN, VAN and VPN connectivity platforms have been identified.	
Identify potential entry points where viruses could enter, including e-mail systems, downloads, infected diskettes, missing patches to operating systems and any lack of testing on standalone equipment of all software before it is installed on the network.	
Determine what virus scanning software is in place, how it determines if files are infected, and how it addresses these (such as, notification, fixes, quarantines) for each platform/environment (such as, firewall, UNIX, PC).	
Obtain and review all policies and procedures related to the malicious code, including, but not limited to the following: • Definition and dissemination • Awareness training for users, network and system administrators and help desk analysts on how to use software, avoid spreading of viruses, and procedures that must be taken when a virus is suspected - Users are required to shut down PCs at least weekly, if antivirus software upgrade requires - Users cannot disable antivirus software on their desktop • Implementation of newly-acquired or new version of software • Implementation of software (system and application) patches and fixes • Maintenance of antivirus software is always current • Security policies for system accounts (such as, administrator, guest)	

• Security policies for all accounts/IDs (such as, length of passwords, periodic change of passwords, password history, expiration period, lockout, password strength) • PC and network configuration standards (possibly use of enterprise configuration management tool) • Application standards • E-mail standards • Assignment of responsibility to enforce these policies and procedures	
Evaluate vulnerabilities and security risks by performing specific tests, for example: • Select some network drives and run the antivirus detection software to see if any network servers have infected files. • Discuss with the NT administrator which services are running on the NT server, and the reason this is deemed appropriate. • Select sample of desktops/PCs (and laptops) and validate that the antivirus protection software is appropriately and adequately installed, and is the most current version (such as, check that the user cannot or has not disabled the virus protection software). • Determine if the virus signatures loaded are the most current version. • Select a sample of desktops/PCs (and laptops) and run the antivirus protection software to see if any PCs have infected files. • Query end users on knowledge of antivirus policy. • Obtain the third party antivirus policy and configuration, and evaluate for appropriateness.	
Determine accountability and timeliness to enforce any procedures that are in violation.	
Provide reasonable assurance that procedures to address an incident have been defined and are used.	

Review documentation of incidents reported during selected timeframe to verify that: • Appropriate managers were informed • Details were documented • Spread was minimised • Incident reports were communicated to other users • Viruses were eradicated • Incidents were investigated • Incidents were appropriately addressed • Preparations for reoccurrence were made • The network is monitored for unusual activity	
Review virus removal process, which should include the cutting off of Internet access, using scanners and detectors, checking the start-up files, checking memory, looking for Trojan ports and deleting Trojan files and e-mail worms.	
Rights for all accounts/IDs should be reviewed for high-level privileges to provide reasonable assurance that these are limited to those whose job responsibilities require this level of access, if a data security audit has not been performed recently. Also, provide reasonable assurance that these require strong passwords, and other similar controls (i.e., access to powerful utilities is limited).	

4. REPORTING

4.1. Suspected infection

4.1.1. Each user is responsible for their own asset (computer and peripherals). When an infection due to malicious code is suspected the user should immediately stop computing and follow the emergency procedure provided by management and/or the security officer. In addition he/she should inform the appropriate parties (security department, help desk, etc.) about the problem in order to mitigate consequences and probability of malicious code propagation within the organization. If the user is not able to follow the procedure,

he/she should immediately power off the computer and call the appropriate party (security department, help desk, etc.) for assistance.

5. EFFECTIVE DATE

5.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

P6
1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.”

1.1.2 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.3 G25 Review of Virtual Private Networks provides guidance.

1.1.4 P3 Intrusion Detection Systems (IDS) Review provides guidance.

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement How well is the IT function supporting business requirements?
- IT control profiling What IT processes are important? What are the critical success factors for control?
- Awareness What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 Primarily intended for IS auditors—internal as well as external—this document can be used by other IS security professionals with responsibilities in firewall configuration.

1.3.2 Modern businesses are organised as a set of core processes operating within supply and demand networks. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper processes. These increasingly complex operating networks are supported by available communication technologies (mainly the Internet), allowing businesses to focus on their core competencies and partner with others to deliver enhanced value to customers.

1.3.3 The transformation of the old processes is enabled by new communication channels. These channels provide new linking possibilities among different systems and networks, making them available to more people and letting the entities and their processes interact, such as, e-procurement and e-sourcing.

1.3.4 These new processes have shown the necessity for new techniques to allow authorised access to an organisation’s data and programs and protect them from unauthorised (and mostly malicious) access through the new channels that interconnect the existing networks with external sources. In light of this, equipment has been developed with special kinds of functionality (firewalls) that help to minimise the previously mentioned risks.

1.3.5 There are various types of firewalls and they are used in several different configurations, each one suited for a specific protection need.

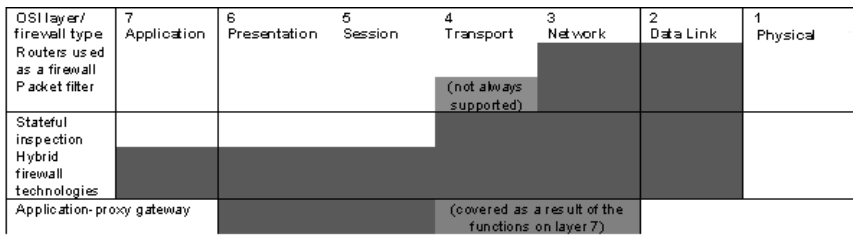
1.3.6 This document gives some guidance for IS auditors who are being increasingly faced with having to audit or review new processes that interconnect different entities through means such as the Internet, direct connections and leased networks, and thus evaluate the

strength of the protection barriers to provide reasonable assurance of information integrity, availability and confidentiality.

2. FIREWALLS

2.1 Types of firewalls

Note: OSI is an acronym for open standards interconnection.

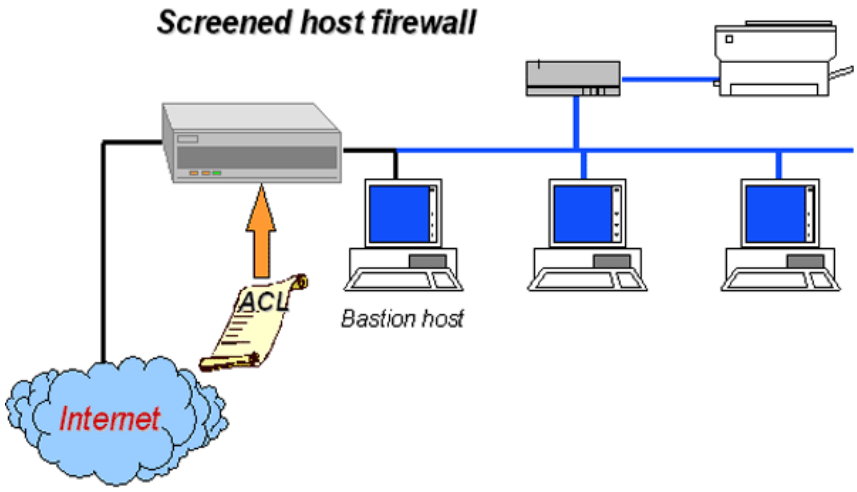


2.1.1 Network layer firewalls generally make their decisions based on the source, on destination addresses and in individual IP packets. A simple router is the "traditional" network layer firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or from where it actually came. Modern network layer firewalls have become increasingly sophisticated and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. An important distinction about many network layer firewalls is that they route traffic directly through them, so to use one you either need to have a validly assigned IP address block or to use a "private Internet" address block. Network layer firewalls tend to be very fast and tend to be very transparent to users.

2.1.2 Screened host firewalls control access to and from a single host by means of a router operating at the network layer. The single host is typically a bastion host—a highly defended and secured strong-point that can resist attack.

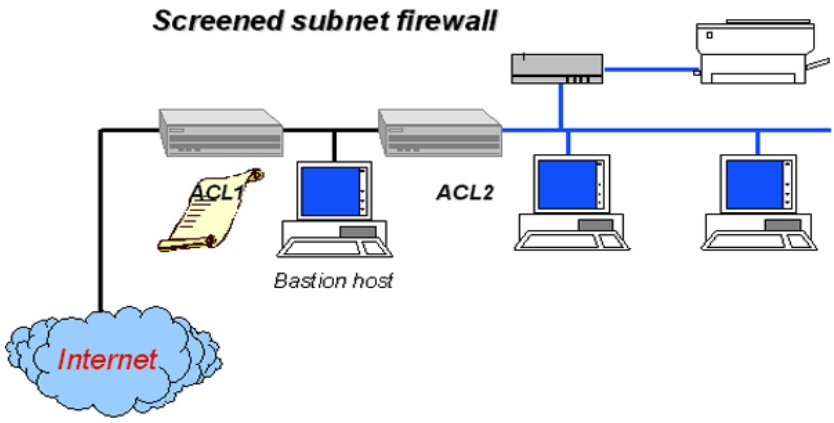
The Internet	Exterior Router	Bastion Host	Internal Network	Trusted Devices
traffic »	traffic »□□	traffic	traffic □□□	traffic «

		□□□		



2.1.3 Screened subnet firewalls control access to and from a whole network by means of a router operating at a network layer. It is similar to a screened host, except that it is, effectively, a network of screened hosts.

The Internet	Exterior Router	Bastion Host	Perimeter Network	Interior Router	Internal Network	Trusted Devices
traffic □□	traffic □□□	traffic □□□			traffic □□□	traffic □



2.1.4 Packet filter firewalls (perimeter solutions) examine all the packets they see, then forward or drop them based on predefined rules. Packet filtering uses source/destination, protocol and port information from the packet header to restrict the flow of traffic. The packet filtering firewall is perhaps the most common and easiest to employ for small, uncomplicated sites. However, it suffers from a number of disadvantages and is less desirable than the other firewalls. Basically, a packet filtering router is installed at the Internet (or any subnet) gateway and then the packet filtering rules are configured in the router to block or filter protocols and addresses. The site systems ordinarily have direct access to the Internet while all or most access to site systems from the Internet is blocked. However, the router could allow selective access to systems and services, depending on the policy. Ordinarily, inherently dangerous services such as NIS, NFS, and X Windows are blocked. Packet filter firewalls can be found on TCP/IP based networks but also on other networks using layer 3 addressing (for example, IPX). Some routers also can provide some basic functions over layer 4, becoming a simple implementation of a stateful inspection firewall. As the filtering rules they use are very simple, they allow fast processing speeds, but at the same time, this feature makes them very susceptible to misconfiguration by defining a set of rules that does not comply with the organisation's security policy. As they do not examine higher layers of data, they are not suited to protect against attacks made using application function, nor can they protect effectively against spoofing attacks. They also have a limited logging capability. This type of firewall is used in environments that require high processing speeds, but no complex logging or

authentication functions. This functionality can be included as the only firewalling feature (for example in a router) or may be one among others that operate at higher layers.

The Internet	Firewall	Internal Network	Trusted Devices
traffic »	Traffic »□□	traffic □□□	traffic «

2.1.5 Stateful inspection (or dynamic packet filtering) is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet to determine more about the packet than just information about its source and destination. It uses a combination of packet filtering, stateful inspection and proxy servers. SI/DPF uses state tables and programmed instructions to analyse information from the packet header and from the contents of the packet (application state), up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. These devices examine the packets, remember which connections use which port numbers, and shut down access to those ports after the connection closes. The expressions that define the filters have to be written under the vendor syntax. Stateful inspection/dynamic packet filtering is an extension of the firewall operating system that stores application state and packet header information in a table. That table is used to classify traffic and to apply different processing rules to established connections and to manage opening and closing specific ports.

2.1.6 Hybrid firewalls combine aspects of packet filtering and application-level filtering. Like packet filtering, these firewalls operate at the network layer of the OSI model, filtering all incoming packets based on source and destination IP addresses and port numbers, and determine whether the packets in a session are appropriate. They also can act like application-level firewalls in that they can review the contents of each packet up

through the application layer. Ordinarily they employ some combination of security characteristics of both packet filtering and application filtering products. A hybrid firewall uses a combination of packet filtering, stateful inspection and proxy servers. The objective is to process different types of traffic according to the risk they present and to balance processing time against throughput. In a hybrid implementation, some hosts are behind a traditional firewall, while other hosts live on the outside. An IPSec gateway at the central site provides connectivity to the outside machines. This configuration is common at organisations with a major central site and some number of telecommuters. As in ordinary virtual private networks (VPNs), remote hosts have full access to the inside by virtue of the IPSec tunnel. Traffic from inside machines to the remote nodes is similarly protected. What is distinct is that traffic from remote nodes to the rest of the Internet is governed by the central site's security policy. That is, the firewall administrator distributes a security policy to the remote nodes. Ideally, of course, this same policy statement is used to control the traditional firewall, thus ensuring a consistent security policy.

2.1.7 Proxy server firewalls run special software written to allow specific programs to function and to enforce authentication, filtering and logging policies. For example, an HTTP proxy is written to specifically allow HTTP access, and only HTTP access, through it. It also requires special action to be taken at the user level. For example, in Netscape, the user must edit the properties dialog—specifically, go into "Advanced," then go into "Proxies," and make the appropriate entries there. As they have no firewall capabilities, they have to be placed behind a firewall. A user who needs to access external resources should use the proxy server that can enforce user authentication, log user activities and can scan, for example, web and e-mail contents. Additional supported functions are content scanning, service blocking, virus removal, etc. Proxy server firewalls typically act as an intermediary for user requests, they set up a second connection to the desired resource either at the application layer via application proxy or at the session or transport layer via circuit relay. They intercept all messages entering and leaving the network. The firewall only allows external systems to communicate with the proxy server. The proxy server effectively hides the true network addresses.

External Host	The Internet	Firewall	Dedicated Proxy Server	Internal Network	Trusted Devices
Traffic »	traffic »	traffic »□□	traffic »□□	traffic □□□	traffic «

Advantages of proxy server firewalls:

- The proxy ordinarily is highly aware of the data format it handles, and can look for many inconsistencies, and provide protection from them.
- Only specific protocols that are to be supported are allowed.

Disadvantages of proxy server firewalls:

- For any new protocol(s) that are allowed, a proxy that is specifically aware of that protocol is necessary.
- If an existing protocol is extended, proxy software will probably need to be updated.

Proxy server firewall provides a controlled network connection between internal and external systems. A virtual circuit exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server. Responses are then received by the proxy server and sent back through the circuit to the client. While traffic is allowed through, external systems never see the internal systems. This type of connection is often used to connect "trusted" internal users to the Internet. Used most often for outgoing connections that relay TCP connections and are transparent to the user. During a call, the gateway's relay programs copy bytes back and forth; the gateway acts as a wire.

Auto-connect capability, i.e., external hosts outside the gateway, need access to a printer on the inside. Restrictions on port designation and access control are implemented. Auto-connect assists with connection control, if a hole in the external host is created. Manual servicing is a protocol for the connection service that needs to be implemented to define

the desired destination. Either a proxy (destination hostname) or SOCKS (IP address) is implemented. The logs store the bytes and TCP destination but do not examine them.

Advantages of auto-connect proxy firewall servers:

- More secure than a packet level gateway, although not as secure as an application gateway
- Replay TCP connections
- Permissions granted by port address
- Is capable of understanding the contents of the packet

Disadvantages of auto-connect proxy firewall servers:

- Inbound connections are inherently risky. They relay packets without inspection, have limited audit capabilities and no application specific controls
- No application-level checking

2.1.8 Transparent firewalls are amalgams of proxy server firewalls and network address translation (NAT) (see 4.1.1). An internal machine only has to know where to send packets to reach the outside, similar to a NAT firewall. However, the firewall may transparently invoke proxy-like mechanisms on certain traffic, for security purposes, rather than just blindly forwarding them through. The internal machines may or may not have a private IP address range.

Advantages of transparent firewalls:

- No special configuration on the client side, just like a NAT firewall
- Allows for finer control and protection for well-known services

Disadvantage of transparent firewalls:

- Shares most of the disadvantages of a NAT firewall. If a particular application protocol is being used on a non-standard port, all "special" protections are lost. Depending on the rules allowed, it may not even happen at all.

2.1.9 Application-level (gateway) firewalls have all the functionality of the dedicated proxy servers, plus the functionality of a firewall (i.e., each proxy application can access the firewall rule base to permit or deny packets). They are generally hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them, as they can inspect all the packets (destination address, ports and packet contents). They can implement enhanced authentication methods, as they can combine more information (they can consider additional information than packet filter and stateful inspection packet filter firewalls, that authenticate users based on the network layer address that it is easily spoofed). Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may effect performance and may make the firewall less transparent (in high-bandwidth applications a dedicated proxy server behind a firewall is often a preferred solution). An application-layer firewall, called a dual-homed gateway, is a highly secured host that runs the proxy software. It has two network interfaces, one on each network, and blocks all traffic passing through it.

The Internet	Firewall (Dual Homed Host)	Internal Network	Trusted Devices
traffic »	traffic »□□	traffic □□□	traffic «

Advantages of application-level (gateway) firewalls:

- Easier to log and control all incoming and outgoing traffic
- Application layer firewalls can incorporate encryption to protect traffic transmissions

Disadvantages of application-level (gateway) firewalls:

- Administratively intensive—each networked service requires separate configuration (i.e., HTTP, telnet, mail, news)
- Inside users must use proxy-aware clients for most services
- Without further modifications to a service client, the user would have to connect to firewall. Modifications can be applied to make this connection transparent to the user

3. COMMON FUNCTIONS AND FEATURES RELATED TO FIREWALLS

3.1 Network Address Translation

3.1.1 NAT is a tool for "hiding" the network-addressing schema present behind a firewall environment. It allows a chosen addressing schema to be deployed behind a firewall, while still maintaining the ability to connect to external resources through the firewall. It also allows the mapping of nonroutable IP addresses to a smaller set of legal addresses. Network address translation can have three modes:

- Static NAT—Each internal system on the private network has a corresponding external, routable IP address associated with it. With this technique, it is possible to maintain the ability to provide selective access to external users (an external system could access an internal server and the firewall would perform mappings in either direction, outbound or inbound).
- Hiding NAT—All internal IP addresses are hidden behind a single IP address. The main weakness of this configuration is that it is not possible to make resources available to external users once they are placed behind a firewall, as mapping in reverse from outside systems to internal systems is not possible, so systems that must be accessible to external systems must not have their addresses mapped. In this type of implementation, the firewall must use its own external interface address as the substitute or translated address, impairing the flexibility of the configuration.

- Port address translation (PAT)—Similar to hiding network address translation, but with some differences. That is, it does not require use of the IP address of the external firewall interface, and the access to resources behind a firewall system can be granted selectively by forwarding inbound connections on certain port numbers to specific hosts.

3.1.2 Advantage of NAT:

- Requires no special configuration on the client side, except for normal routing configuration. Clients just have to know their default gateway.

3.1.3 Disadvantages of NAT:

- There is no additional security beyond selecting “allow this type of traffic.” Once an internal client connects via an allowed protocol, anything can happen within the bounds of that protocol.
- There is no way to allow for special protocols that require a return connection to be made.

3.1.4 If certain types of protocols are to be restricted, access can be limited to certain ports. On the one hand, this is too restrictive, because internal users may not be able to access web servers on nonstandard ports. And at the same time, this is too permissive, because there may be a disallowed service running on a nonstandard port on the outside, and internal users will be able to access it in this case.

3.2 Intrusion Detection Systems (IDS)

3.2.1 These systems are designed to notify and prevent unauthorised access to a networked system or resource. Often they interact with firewalls to generate an automatic response against a perceived threat (e.g., blocking the source of the attack).
3.2.2 Attack recognition and response software works by continually monitoring network traffic and looking for known patterns of attack. When the software detects unauthorised activity, it responds automatically with some form of defined action configured by the

administrator.

3.2.3 Requirements for a good intrusion detection system are:

- Installable throughout the overall network to ensure enterprisewide security
- Monitor incoming and outgoing traffic
- Provide protection for LANs, Internet, intranet and dial-up access
- Generate alarms in real time to appropriate personnel, such as administrators and security officers
- Configurable to automatically eliminate the intruder and block the intruder's reentry
- Selectively log session data
- Provide audit trails to help reconstruct the attack, for post-investigative analysis
- Can be administered remotely, and can encrypt the administration sessions for security purposes (if required by the client organisation)

3.2.4 Intrusion detection systems are not able to assist in:

- Compensating weaknesses in network protocols
- Analysing all the traffic on a busy network
- Dealing with some of the modern network hardware and related features
- Compensating for weak identification and authentication mechanism(s)
- Compensating for problems in the quality or integrity of information the system provides
- Conducting investigations of attacks without human intervention

3.2.5 The installation of an IDS should be made first by establishing the network perimeter and identifying all possible points of entry. Once identified, IDS sensors can be put in place, configured to report to a central management console. Possible placements are suggested as follows:

- Between the network and extranet

- In the DMZ (demilitarised zone, see section 5.2) before the firewall to identify the attacks on servers in the DMZ
- Between the firewall and the network, to identify a threat in case of the firewall penetration
- In the remote access environment
- If possible between the servers and the user community, to identify the attacks from the inside
- On the intranet, FTP and database environments

3.2.6 Intrusion detection systems can be classified in two categories, host-based and network-based. The effectiveness of network-based intrusion detection is ordinarily greater than host-based intrusion detection, due to its ability to monitor multiple systems and resources. These types of systems ordinarily generate false attack identification, needing human intervention to determine the real attacks. Definitions of the two categories of IDS are as follows:

- Host-based intrusion detection Highly integrated with the operating system, it should be installed on each individual computer system that is to be protected. There are some issues that arise from the use of this type of system: -They have a negative effect on system performance. -They do not provide effective detection over network-based (for example, denial of service). - They can affect system stability
- Network-based intrusion detection Analyses protocols, monitoring network traffic looking for specific strings that could indicate certain types of attacks. The issues that arise from the use of this type of systems are: - In most cases, they can not effectively detect signatures that are distributed among several packets. - They ordinarily require special equipment configurations (feature sometimes not supported) to establish promiscuous mode network interface.- They can be detected by identifying promiscuous mode network interface.- Sometimes it is difficult to predict the signature that identifies an attack.

3.3 Virtual Private Networks (VPN)

3.3.1 A virtual network is constructed in an encrypted or unencrypted form on top of existing network media, to establish secure network links across networks that are not trusted (for example the Internet). This technology can be used to provide secure remote access to corporate networks or link networks between different organisations. The most common protocols used are:

- IPSec
- PPTP (Microsoft Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)

4. COMMON FIREWALL CONFIGURATIONS

4.1 Common Firewall Configurations Uses

4.1.1 Most common uses of firewalls are:

- Control access for internal and external networks (perimeter firewalls)
- Control access among public accessible and public inaccessible servers (DMZ firewalls)
- Control access among internal networks with different access and security requirements
- Control access thru pools of modems and private dial-up networks
- Control access to and from third party administered hosts and networks
- Encrypt internal and external networks that transmit sensitive data
- Hide internal network addresses from external networks (NAT)

4.2 Demilitarised Zone (DMZ)

4.2.1 A DMZ greatly increases the security of a network, protecting any computer that needs to be available from an external network behind one firewall and adding a layer of protection between the shared machine and the internal network. If appropriately configured, there are two protection layers for an attacker to compromise to get to anything valuable.

4.2.2 This type of configuration greatly increases the skills required by an external hacker to compromise the internal network and thus lowers the threat of the internal network being compromised. To further reduce risk, usage of different compatible technologies reduces the chances of exposure.

4.2.3 In a DMZ network, the untrusted host is brought “inside” the firewall, but placed on a network by itself (the firewall host then interconnects three networks). This increases the security, reliability, and availability of the untrusted host, but it does not increase the level of trust that other “inside” hosts can afford. Other untrustworthy hosts for other purposes, such as a public web site or FTP server, can easily be placed on the DMZ network, creating a public services network.

4.2.4 Sometimes a single firewall with three network interface cards is used to implement a DMZ. One of the cards is attached to the external network, the second to the internal network, and the third to the DMZ network. This configuration does not prevent against service degradation effectively during a denial-of-service attack.

The Internet	Firewall	DMZ (dual-homed) eth0/eth1 (SMTP/WWW/DNS, etc.)	Internal Network	Trusted Devices
traffic »	traffic »	traffic »	traffic	traffic «

4.2.5 Advantages and considerations of DMZs:

- Price of the hardware and software of the extra machines needed to implement a DMZ
- Slight decrease in performance
- Cost of the time to implement the DMZ
- Cost of down time the system suffers from adding on the DMZ
- Lowered level of accessibility to an attacker

4.3 DMZ with Dual Firewall Configuration

4.3.1 The organisation's internal network is further isolated from the untrustworthy network by adding a second firewall host. By connecting the untrustworthy network to one firewall host, the organisation's internal network to the other, and the DMZ between, traffic between the internal network and the Internet must traverse two firewalls and the DMZ.

4.3.2 In a more comprehensive definition, consider an Internet protocol (IP)-based infrastructure between an external network (the exterior) and an internal network (the interior). Such an infrastructure typically contains different types of machines: network devices (i.e., routers); systems (i.e., servers running applications, such as e-mail or a web service), and, of course, security appliances (i.e., firewalls). Each firewall interface is considered to represent a different segment of the infrastructure, which is called the DMZ network.

4.3.3 In each of these architectures, firewalls are used to control access at the border of the network mainly for the purpose of protecting the network from an untrusted network. Firewalls deployed entirely within the network can also be used to provide mutual protection among subnets of the network. Controlling access between internal subnets is no different than controlling access between a network and the Internet, so all of the above architectures can be used as internal firewall architectures as well.

4.3.4 In a multiple-layer architecture the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them. This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defences being implemented. Although more costly, it is prudent to use different technologies in each of these firewall hosts. This reduces the risk that the same implementation flaws or configuration errors may exist in every layer. This approach will reduce the chance of redundancy and greater possibility of compromise. The most common design approach for this type of architecture is an Internet firewall composed of two hosts interconnected with one DMZ network.

4.4 Proxy Server

4.4.1 Proxy servers are used in environments that require stronger authentication methods and good logging functions, as each proxy agent is able to require authentication of each individual network user. On the other side, these enhanced security capabilities require more processing power, and thus makes them unsuitable for environments with high-bandwidth requirements. A special agent for the traffic of each application is required on the firewall. They can analyse e-mail and web content by:

- Java applet, ActiveX control, JavaScript filtering
- Blocking some MIME types
- Virus, and macro virus scanning
- Application command blocking
- User-defined blocking functions

5. RISKS CONTROLLED BY FIREWALLS

5.1 Attacks Based on Software Weaknesses

5.1.1 The objective of this type of attack is to put the server on a virtual offline condition (denial of service attack, DoS), but unauthorised access could also occur.

5.1.2 Buffer overflow is probably one of the most effective types of attack. It is not associated with a particular application and it uses publicly known bugs or weaknesses of the software to generate an error condition in the program used to handle a service. The most common origin of the problem is when portions of memory used by the program are rewritten by an overflow condition. An example of an attack using this weakness is the one made by the virus Code Red.

5.1.3 Directory transversal attack is directed against web servers, trying to access the file systems outside the authorised pages. This can result in unauthorised access to data, or execution of unauthorised code. In some of the oldest versions of the software, using an

URL in the form of http://server/../../ was enough. An example of an attack using this weakness is the one made by the virus NIMDA.

5.1.4 Source disclosure attack is directed against web servers that process dynamic pages. They try to access their source code that can include installation information, such as user IDs and passwords to access databases. This form of attack can be made issuing a special URL that the server processes incorrectly, or makes the server execute some software components that can contain errors or bugs.

5.1.5 MIME exploit attack is directed against mail clients and services and, in some cases, against browsers. The attack consists of the modification of headers to provoke certain situations, such as DOS, program executions. Some of the controls that can be in place are:

- Continuous follow-up of published bugs and weaknesses, and installation of patches and software updates
- Procedures to control system and application logs to detect attacks

5.2 Attacks Based on Processing Power

5.2.1 SYN floods are intended to generate an error in the program used to handle the service. In their simplest form, they overwrite memory used by data or program code and thus generate the error. In more dangerous forms, the attacks manage to execute program code provided by the attacker. As the services are ordinarily executed at a high level of privilege, these types of attacks are high risk. Ordinarily, packets include false origination addresses. SYN floods generate two basic problems—bandwidth shortage and growth of the connection table on the server. Controls that can be put in place against this type of attack (although they cannot have a total effectiveness) include:

- Configuring firewalls to detect and filter spoofed addresses
- Adjusting connection parameters, such as number of waiting connections and timeouts, to avoid excessive growth of connection table

5.2.2 UDP flooding is similar to the previous case. The main difference is that UDP does not use the concept of connections. The attack is based on the occupied bandwidth and, eventually, in the resources used by the server to answer the packets.

5.2.3 ICMP floods have been some of the most effective past attacks. They use the configuration problems to enhance the attacks. One of the most well-known applications, Smurf, is based on using other networks to attack the final target.

5.2.4 DdoS attacks intend to flood the target site with one or more attacks of DoS. It does not use software bugs or configuration errors. The attack ID is based on a massive use of bandwidth and requires that many previously affected nodes of the network (hundreds) participate in the attack. There are not so many options to prevent this type of attack. Some of the controls that can be in place are:

- Packet filtering
- Providing reasonable assurance that weaknesses of interconnected sites are as well controlled as they can be
- Adjusting parameters to control excessive connection table growth

6. PROCEDURES TO REVIEW FIREWALLS

	Suggested Procedures	
Gather preliminary information—These are examples of information that can be obtained to plan the audit work.	• Obtain security policies. • Obtain the firewall security policy. • Identify the services that the firewall is intended to protect and perform a high-level risk assessment of their sensitivity considering the seven information criteria defined by COBIT. • Identify the risk assessment process in place to identify the main sources of threats and the probability of their occurrence. • Develop an understanding of how the technology is being used, including the security measures in place, such as authentication methods, security administration and hardware maintenance.	

	• Identify procedures used in the systems development life cycle, for the set of applications used from the outer network (those accessed directly and the ones they use thru interfaces) and for the system software of the firewall. • Determine the logging functionality in place. • Identify the procedures used for rule base maintenance. • Identify the procedures used to monitor new bugs or weaknesses of the software used. • Identify the procedures used to review systems and application logs to detect attacks. • Identify the procedures to share technical and security incident related information with neighbor sites. • Identify the configuration management procedures.	
Risk assessment	• Adjust the scope of the review using the information on sensitivity of the services that the firewall is intended to protect, the identified risks, and the likelihood of their occurrence.	
Detailed planning All the control objectives that can be identified as a result of selecting COBIT processes can be reviewed by usual installation reviews. This section includes some special procedures that can be included as a part of a firewall installation review. These are examples of areas to	• For the IDS installation, review the analysis made to evaluate the existing network, the identification of entry points, the types of traffic allowed by firewalls, the analysis rules introduced, and the alarms and notification schema set. • Review each DMZ on an individual basis, while considering the others as a different network or computer as applicable. In this approach, the configuration and rules should be considered against all the types of traffic of the networks related to the DMZ. • Review the procedures used to monitor security-related sources of information (mainly web sites and specialised sources) and identify new types of attack, such as software bugs; consider verification of whether all available security patches have been applied. • Review the systems development life cycle controls in place over	

include in the review.	the code executed as part of the firewall software and the applications published to the outer side of the network, such as segregation of duties, initiation and testing. • Review the authentication controls used to control access from the outer network. • Review the procedures used for device administration (including at least physical access and administrators' passwords, for example, to reduce the risk of tampering the connections thru unauthorised access. • Review the procedures used to control remote access for administering network devices (by administrators or vendors). • Review the procedures to review the logs in an effective and timely manner and to deal with potential harmful traffic. • Review the procedures for dealing with potential or effective attacks. • Review the procedures for rule-base maintenance, such as reviewing access to maintenance functions, request procedures, new or modified rules testing, transfer to production and documentation. Determine if there is a formal and controlled process in place to request, review, approve and elevate firewall addition and changes into the production environment. Specifically: 1. Determine if the formal request includes the business purpose and sponsor, date it is requested and how long (in time duration) the rule will be needed. 2. Determine if the review is completed by technically competent individual who understands the risk associated with the rule. The reviewer should document the risk in relation to the protection of the entire information infrastructure. 3. Determine if the approval includes both the head or supervisor of the firewall administrator and the appropriate business manager. The	

	approval of the firewall rule request must be done formally. 4. Determine if the firewall rule is formally tested first in a test environment prior to elevation into the production processing environment. Where possible, test for outage of services (for example identifying unusual amounts of off-hours made by the unit where the change was requested). • Review risk management procedures. • Identify the existence of single points of failure. • Review virtual private network in place (see guidance on Virtual Private Networks from ISACA). • Review the plan for conducting penetration tests and the criteria for re-performing the tests when changes are made. Coverage of the risks identified by the tests. • Identify the filtering rules in place (to determine if they address all the issues included in the security policy and other applicable threats identified during the risk analysis). Verify that the overall firewall rule restrict access, unless specifically allowed by the rules. • Review the procedures to test revised rules prior to the transfer to production environment. • Review physical access controls to firewall and network equipment that connects it to the networks. • Review the procedures used to test new software and configure its security to accomplish defined security policies. • Review disaster recovery and contingency procedures. The existence of a fail-over device to back up the processing functions of the firewall should be considered (as its services ordinarily have high-availability requirements). • Review configuration management processes.	

Stateful inspection/ dynamic packet filtering (SI/DPF)	• Document how SI/DPF will affect the controls provided by the other firewall when the SI/DPF is used as the border firewall and there is another firewall behind it.
	• Confirm that program change controls (specially testing controls) are applied to any API if APIs in SI/DPF are used (to execute code written by the organisation by the firewall operating system).
	• SI/DFP uses state tables and programmed instructions. It uses information from the packet header and from the contents of the packet, up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. Design and perform testing of traffic that will be affected by SI/DPF, to verify its proper functionning.
	• Examples of aspects to consider when reviewing filters—gateways, FTP sessions, X Windows, DNS, fixed addresses. Confirm that:
	  o It only allows access to those addresses intended to be accessed from the outside
	  o Does not allow use of unauthorised services, such as FTP and Telnet
	  o Does not allow to access certain ports
	  o Only allows packets that come from authorised sites from the outer network
	  o Discard all source-routed traffic
	• Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.
	• Confirm that there are rules in place to avoid IP spoofing.
	• Confirm that if NAT is used, only those packets that come from certain allowed IP addresses in the internal network are passed, and	

	that incoming traffic is only allowed when a valid connection is established.	
Packet filtering	• When the router is used as the border firewall and there is another firewall behind it, document how it will affect the controls provided by the other firewall. Obtain (or create) an understanding of how packet filtering is being used to filter the packets in terms of the use of source/destination, protocol, and port information from the packet header. • Assess the effect on controls and identify the key areas of risks created by the use of packet filtering. Confirm that: o It only allows access to those addresses intended to be accessed from the outside o Does not allow use of unauthorised services, such as ftp and telnet o Does not allow to access certain ports o Only allows packets that come from authorised sites from the outer network o Discard all source-routed traffic • Design and perform testing of traffic that will be affected by packet filtering. Evaluate rules that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices. • Confirm that there are rules in place to avoid IP spoofing. • Confirm that if NAT is used, routing to internal IP addresses cannot be made directly.	
Inherent risks of packet filtering	• There is little or no logging capability, thus an administrator may not determine easily whether the router has been comprised or is under attack • Packet filtering rules are often difficult to test thoroughly, which	

	may leave a site open to untested vulnerabilities. • If complex filtering rules are required, the filtering rules may become unmanageable. • Each host directly accessible from the Internet will require its own copy of advanced authentication measures.	
Hybrid firewalls	• Document how the use of the hybrid firewall will affect the controls over network traffic. • Obtain (or create) an understanding of how the three firewall approaches are being used (packet filtering, stateful inspection and proxy servers). Determine the logic for passing traffic into each of the firewall's processes. • Assess the effect on controls and identify the key areas of risks created by the use of a hybrid approach. Assess the decision logic applied to determine which firewall approach will be applied to each type of traffic. • Design and perform testing of traffic that will be affected by SI/DPF, considering the following rules: o Confirm there is consistency in sending similar protocols to the same process within the hybrid. o Confirm that any API's used in stateful inspection are controlled. o Confirm the proxy process is maintaining the separation between the traffic and the application. o Confirm the balance between throughput and control processing is appropriate. • Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
Proxy firewalls	• The proxy firewall could be a separate device, or a service running	

	on a multipurpose firewall device. Its purpose is to add special processing controls to one type of traffic. • Obtain (or create) an understanding of the use of the proxy—which traffic is being sent through the proxy and which devices are receiving the output. • Confirm that all traffic of the type being processed by the proxy must flow through the proxy firewall. For all devices on the inside of the proxy, confirm traffic of the type being proxied is only accepted from the proxy device address. • Design and perform testing of traffic that will be affected by the proxy, considering the following: o Confirm all traffic is directed to the proxy o Confirm that all traffic of the type being proxied is only processed from the address of the proxy. • Evaluate the procedures for the review of logs from the proxy and the effectiveness of procedures to address potential problems identified from the logs.	
DMZ—Consider a DMZ network with three segments: one embodies the connection to the exterior, one embodies the connection to the interior, and one, the DMZ segment, consists of the IP subnet on which reside systems that can be accessed from the exterior.	• Verify the firewall is invisible to the exterior. • Verify systems on the DMZ segment are invisible to the exterior. • If external service providers can troubleshoot devices at the edge of the DMZ network where connectivity with the service providers (and with the exterior in general) is made, confirm that: o Tests have identified the precise extent to which what is in the DMZ network may be mapped and o The potential exploitation effect is understood. • Review the DMZ network to provide reasonable assurance that external entities cannot administer or configure: o The firewall o Network devices and systems in the DMZ Network (If	

network devices on the external facing segment, such as routers that connect with service providers, can be accessed for any reason, such as troubleshooting, verify controls exist over who can administer/configure these devices.)

- Verify access control rules are set up in network devices on the external facing segment for the purpose of denying packets that represent undesirable communications, such as denial-of-service attacks.
- Review firewall rules to verify every packet is by default denied unless a specific rule exists to permit the packet to proceed but only to a destination system in the DMZ segment.
- Confirm systems on the DMZ segment are set up so they cannot communicate with any other system outside the DMZ segment except through the firewall. If exceptions exist, evaluate the specific risks, the justification, and the compensating controls.
- Confirm systems on the DMZ segment are set up so that they cannot initiate communications with the interior. Again, if exceptions exist, evaluate the specific risks, justification and compensating controls.
- Confirm network devices, firewalls and systems on the DMZ network are configured so that routing between any possible combination of devices, firewalls and systems is well defined:
    - All routes into, through and out of the DMZ network are easily identifiable.
    - The routing set up is the minimum needed to support authorised communications flows. (If nonroutable communications protocols are used, confirm they have a purpose consistent with security policy requirements for the DMZ network.)
- If NAT is used, provide reasonable assurance it works in a manner consistent with security policy requirements and that the

configuration is periodically recertified by accountable individuals.

- Confirm the firewall is set up:
  - To deny all packets entering from the exterior with source IP addresses set up for internal networks.
  - To deny all packets coming from the interior with source IP addresses not set up for the interior.
- Confirm firewall rules discover external attempts to scan for commonly scanned ports (regardless of whether systems actually exist to listen on such ports).
- Confirm the firewall is set up so that no message is returned in reply to any incoming packet that is denied.
- Confirm the firewall has been tested by scanning every segment, including the DMZ segment, from every other segment to identify what packets can and cannot get through. Provide reasonable assurance the results are consistent with the overall security policy.
- Confirm every rule in the firewall is consistent with the security policy. That is, provide reasonable assurance of consistency with policy is verifiable by examining the following components of potentially acceptable packets: protocol, source system IP address, destination system IP address, source port and destination port. For example, the destination system and port combination in a rule should make sense when the function of the destination system on the DMZ segment is considered. A rule should protect the firewall itself; should align with the functions provided by the systems on the DMZ segment; and should permit systems on internal networks to initiate communications with systems on the DMZ segment or allow systems on the DMZ segment respond to communications initiated from the interior. If the rule base has too many rules to be reviewed during the test, it may be an indicator of a poor security architecture design, making it very difficult to administer and to

	ensure proper coverage. • Confirm the rules in the firewall deny all packets that include TCP or UDP ports above port 1023 to provide reasonable assurance the application ports are being used as intended. If not, evaluate the specific risks, justification and compensating controls. • If multiple physical firewalls exist in the DMZ network for high-availability, redundancy or failover purposes, confirm the running configurations of the firewalls are equivalent.	
	Additional key points to consider	
Configuration	• DNS, e-mail, server load balancing services, or any software or services not related to firewall-specific functions should not be installed in or processed by the firewall. • Firewalls should be configured to hide internal restricted DNS information from external networks. • External firewalls should restrict incoming SNMP queries. • Router access control lists do not provide the protection level required for a firewall solution. A router should be used as part of a firewall solution (for example: initial Internet facing filter). This provides connection and removes some of the workload from the firewall by only passing those ports that are required, rather than having the firewall filter every single port. (However, there should still be rules in place to block unused ports on the firewall, just in case.) • Configure firewalls as “fail closed.” • Hide internal network information from external sources. • Configure firewalls to “deny all services, unless explicitly allowed.” • Translate addresses of internal network nodes that are allowed to communicate with external networks. • Avoid UDP-based services when possible.	

	• Scan, filter or block Java, JavaScript and Activex. • Limit NNTP to users that need it. This should be formally justified. • If possible, use static routing instead of routing protocols. • Apply strong security policies to the host where the firewall resides. • Restrict access to firewall generated logs to avoid its deletion or modification in an unauthorized manner. • Apply all security-related patches or similars to the components of the firewall system. • Determine procedures are in place to verify security policies (for example: penetration testing, manual reviews of rule base, OS security reviews, etc.). • Verify integrity monitoring tools for sensitive system files on the firewall system exist.	
Monitor, audit and incident response	• Monitor firewall alerts on a continuous basis. • Log all the firewall activity. • Determine sensitive or high-risk connections have additional protection tools, such as intrusion detection systems.	
Backup and recovery	• Verify continuity plans for firewalls are in accordance with those of other high-availability services, as firewalls ordinarily are components related to services with high-availability requirements.	

P8
IS Auditing Procedure: P8 Security Assessment - Penetration Testing and Vulnerability Analysis

3. TYPES OF PENETRATION TESTING AND VULNERABILITY ASSESSMENT

3.1 Scope of Evaluation

3.1.1 There are several types of penetration tests that will, depending upon the circumstances, affect the scope of the evaluation, methodology adopted and assurance levels of the audit.
3.1.2 The individual (appropriate IT management) responsible for safeguarding the organisation should evaluate various alternatives, selecting that which provides the maximum level of assurance with the least disruption acceptable to the organisation (cost/risk analysis).
3.1.3 There should be agreement on the type of penetration testing to be carried out– intrusive or nonintrusive.

4. EXTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

4.1 Internet

4.1.1 The purpose of Internet testing is to compromise the target network. The methodology needed to perform this test allows for a systematic checking for known vulnerabilities and pursuit of potential security risks. The methodology ordinarily employed includes the processes of:

- Information gathering (reconnaissance)
- Network enumeration
- Vulnerability analysis
- Exploitation

- Results analysis and reporting

4.1.2 There are several variations to the processes listed in section 4.1.1. However, a common, standardised and objective script is ordinarily followed and should provide a detailed and exact method of execution. In addition, the intricacies of new vulnerabilities and methods of exploitation require detailed study with a history of information to draw upon.

4.2 Dial-in

4.2.1 War dialling is the systematic calling of each number in the target range in search of listening modems. Once all listening modems are identified, brute force default password attempts or strategic guessing attempts are made on the username/password challenge (sometimes only passwords are necessary) to gain unauthorised access.

4.2.2 Access to the login screen banner is crucial to accessing any system. Some systems require only a password, which can be a vendor-provided default password or just hitting "enter."

4.2.3 At times of poor configuration, even a login banner does not appear and access is granted directly devoid of any authentication mechanism.

5. INTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

5.1 Goal

5.1.1 The goal of internal penetration testing is to ascertain vulnerabilities inside the network perimeter. The testing performed closely parallels that which an internal IS auditor will be assigned to audit, given the size, complexity and financial resources devoted to risk associated with lack of security concerns. The overall objective is to identify potential vulnerabilities within the internal network and weaknesses in controls in place to prevent and/or detect their exploitation by a hacker/malicious

employee/contractor who may obtain unauthorised access to information resources or cause system disruption or a system outage.

5.1.2 The first phase relates to information gathering, which is comprised of public information search, googling, obtaining maximum information about business, employees, etc., thereby profiling the target. For instance this phase may result in obtaining resumes/CVs of employees which may be useful in understanding technologies employed at the attack site.

5.1.2 The first testing goal is to ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges. This is the network discovery stage.

5.1.3 Once critical points/devices are identified within the network, the next step is to attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices (e.g., UNIX, NT, Apache, Netscape and IIS). This comprises the vulnerability analysis phase.

5.1.4 Exploitation and notification is the third and final phase.

6. PHYSICAL ACCESS CONTROLS TO DATA CENTRE AND OTHER WORK SITES

6.1 Rogue Access Jacks

6.1.1 Identification of telecommunication access paths into and out of the organisation's premises, including communications rooms, and the data centre areas are critical to identifying potential methods to intercept, prevent or modify data communications. These access paths should be physically secured from unauthorised access and rendered inaccessible without the knowledge and specific permission of the organisation as well as specialised equipment.

7. SOCIAL ENGINEERING TESTING

7.1 Tests of Controls

7.1.1 Social engineering techniques are employed in an attempt to obtain information regarding perimeter network devices and their defenses (i.e., IP address ranges, firewalls and default gateways) as well as potential internal targets. The information gathered during the reconnaissance phase outlines the basis of this test. The purpose of this testing is to assess the ease of extraction of critical information from internal organisation resources and employees/contractors, or others with detailed knowledge of the organisation, without their becoming aware of the significance of the information obtained. Of particular interest is testing whether the organisation's help desk will assist an unauthorised or unidentified user.

8. WIRELESS TECHNOLOGY BACKGROUND

8.1 Background and Risks Associated With Wireless Technologies

8.1.1 With the advent of wireless technology for transmitting data and voice, the well-known and relied upon controls instituted using perimeter devices are disappearing. Gone are the physical security controls, such as security guards, cameras and locks, that were effective in protecting wired networks and data transmissions. The major vulnerabilities result from the users of wireless technologies not addressing the following:

- Reliance on WEP for encryption
- Wireless networks not being segregated from other networks
- Descriptive SSID or AP names being used
- Hard-coded MAC addresses
- Weak or nonexistent key management
- Beacon packets that have not been disabled or are "enabled"
- Distributed APs
- Default passwords/IP addresses
- WEP weak key avoidance
- DHCP being used on WLANs
- Unprotected rogue access pointsThe risks and threats associated with attacks against wireless networks are widespread including:

- Attacks where message traffic is captured and analysed and encryption keys cracked, i.e., initialisation vector—IV
- Resource theft, where Internet access is obtained that in return is used as a launch pad for other attacks, i.e., cyclincal redundancy check (CRC-32)
- Denial-of-service due to signal interference and propagation of threat from viruses and worms

8.1.3 In addition, as with other types of technologies, the greatest weakness with wireless security is not the technical shortcomings but out-of-the-box insecure installations. The human factor is typically the weakest link.

9. WEB APPLICATION

9.1 Manual and Automated

9.1.1 Web application testing includes manual and automated testing of the portal site as an outsider with no login information. This testing compliments the external penetration testing. The goal of this testing is to gain an understanding of how individuals interact with the system in accessing sensitive data.

9.1.2 Additional testing may include testing of the portal site by an insider through a standard login account. The goal of this testing is to determine the ease of access to sensitive information that is not authorised by the login account (i.e., privilege escalation).

9.1.2 Identification and exploitation of vulnerabilities can be accomplished through the use of various commercial and open source vulnerability assessment tools.

10. SUGGESTED PROCEDURES

	Suggested Penetration Test and Vulnerability Analysis Procedures	
Planning	• Define the scope based on the nature, timing and extent of the evaluation. • Verify that no test will violate any specific law of local or national statute.	

	Also, the auditor should consider obtaining a signed "authorisation form" from the organisation agreeing to the deployment of penetration testing tools and methods. • Investigate and use available automated tools to perform penetration testing and vulnerability assessments. These tools improve the efficiency and effectiveness of penetration testing. • Define the scope of the review by asking the following questions: o Will the chief information officer, computer security and IT personnel be told of the penetration test? o Will the audit testing focus on detecting control weaknesses from those accessing the information infrastructure from the Internet and dial-in access (external) or from inside the organisation (internal)? o How far into the network and information asset will the penetration testing be performed? For example, will the testing be performed to the extent of actually accessing the information assets or will it occur to an access check point (where access to the information assets is not accomplished but there is sufficient information that it could occur based on testing)? Will the test be intrusive or nonintrusive? o What level of overall system degradation, and for what duration, will be acceptable in performing the tests? o Can the test be performed off hours to avoid potential conflicts with causing critical system outage (e.g., executing nmaps against firewall off hours, such as Sunday morning, while web application services are not used)? • Obtain access to a (public) vulnerability database, such as bugtraQ, packetstorm, etc. The tester should determine that any tools used are up to date with the latest vulnerability database.	
Skills	• Possess sufficient technical knowledge of, and ability to recognise and/or	

Required	detect different types and variations of, security flaws/bugs/weaknesses/vulnerabilities. For example, the individual should have an understanding of the controls required over dial-in penetration, denial-of-service, password cracking, buffer overflows and wireless, as well as have access to up-to-date vulnerabilities database services. • Possess strong knowledge of how various technologies work, such as firewalls and routers, intrusion detection systems, and various types of authentication mechanisms. Possess working knowledge of application programming, such as JAVA, Visual Basic and C++. • Possess knowledge of various operating systems, such as UNIX, Linux, NT/2000, Windows and OS/390 (or its current mainframe version). • Possess working knowledge of TCP/IP and networking protocols. • Possess working knowledge of web server software, including Microsoft IIS and Apache. • Possess knowledge in utilising the penetration tools selected to detect bugs and vulnerabilities. • Possess knowledge of the effect on the internal system of executing penetration and vulnerability tools, including the NMAP, ISS, Whisker, Nikto, WebInspect, AppScan, ESM and Root , Nessus.	
Agreements	• Keep all records, including specific and detailed logging of all keystrokes and verbal discussions, of all activities during the penetration and vulnerability testing. These records should be in sufficient detail to recreate the test, if necessary. • Keep all records of the penetration testing, including the results, confidential as they are the property of the organisation. All records of the penetration and vulnerability testing should be maintained within the organisation’s control. The individual performing the test should sign nondisclosure and code of ethical conduct statements with the organisation	

	regarding the confidentiality of the scope of the test and results. • If the test is to be performed by external consultants, include a contract to protect the organisation. The contract should state the boundaries and scope of the work to be performed, the ownership of the results and test procedures, as well as require confidentiality and ethical conduct of the consultants. In addition, the external consultant should provide insurance and a "hold harmless" clause to mitigate risks as a result of an inadvertent release of information.	
Scope Questions	• Does the testing consist of evaluating the control environment based on penetrating the information infrastructure from inside vs. outside the network perimeter? For example, if the test consists of evaluating the firewall rule set based on attempted access to penetrate the network from the Internet, the evaluation is focused on determining the access control from outside the network perimeter. Testing of perimeter controls is limited in scope to the physical and logical controls that safeguard the information assets from those threats external to the organisation. However, once the perimeter security controls are compromised, a decision should be made, whether to continue testing to determine the adequacy of the controls over the target information systems. Conversely, the vulnerability testing may be focused on evaluating the internal control environment to prohibit access to information assets from inside the organisation. • Is the appropriate level of management, including IT security, notified of the penetration or vulnerability testing? If a formal announcement is made of the testing, strong cooperation and more thorough evaluation may be achieved. Conversely, unannounced testing may better represent the actual risks and management's response based on real-world threats from unauthorised access attempts. It is essential to assess the best-case scenario and level of assurance needed. • Are the individuals performing the test provided information about the	

	organisation in advance? This question goes with whether management is notified of the nature and scope of the test. However, there are times when just the executive or high-ranking IT management is notified of the test and it is not announced to the staff. Nevertheless, if information is provided (i.e., network topology) and used by the tester, a more exact review of the target systems and processes can be examined, possibly resulting in better identification of risks and vulnerabilities. However, providing insider information may result in difficulty in understanding the depth of the vulnerabilities and their likelihood of exploitation. In addition, the IP ranges, if provided by management ,should also be tested.	
Internet Penetration Testing	• Network enumeration is the information obtained: network resources and shares, user logins including generic installation (out of the box) hardware and software vendor user IDs, IDs and their groups, and applications and banners. The steps to consider are: o Identify the domain name, IP address range and other critical information. Ordinarily, the “who is” query is used, which typically provides the address of the target network (i.e., domain name servers and IP address mapping), administrative contact and billing contact. The individual executing the “who is” query should provide reasonable assurance that all listings are obtained, and not just the first 50 items, which may require grouping the names into plurals or modified organisation names. o Identify IP address ranges that may be owned by the organisation. This is typically done by querying Internet number registries such as ARIN, RIP, APNIC and LACNIC. o Identify external e-mail servers by gathering MX record information from DNS servers. o Attempt a zone transfer between all systems identified as a DNS server (including back-up servers) to obtain the network IP listing	

and the machine host names. A zone transfer requests the complete list of matched IP addresses and host names stored within a DNS for a specified domain. In addition, the "nslookup," which is supported by both the UNIX and Windows platforms, may also be used to perform a zone transfer using a DNS server that is authoritative for the domain of interest. In addition, the machine's host names may indicate its purpose (i.e., mail server and firewall), which is one more critical piece of information. Recent technologies prevent the ability to perform a zone transfer without the initiating device.

- Determine whether the organisation has outsourced its domain name function to an Internet service provider (ISP). In cases where this function is outsourced, it is recommended that the terms of the penetration test clearly state whether the hosted system is within the scope of the engagement.
- Notify network staff that a penetration test may be underway because zone transfer can be detected.
- Use ICMP (ping) or TCP ping (with a full or half TCP handshake) sweeps to determine which machines for IP addresses are "up" or "live." Though this step may provide critical information regarding which devices are active, there is a likelihood that perimeter security devices or firewalls may drop the ICMP traffic to the host. It may be filtered and dropped with a response indicating the device is down, when it is not. It is recommended that randomising the order of the IP addresses being pinged helps avoid detection, as does varying the NMAP. NMAP is a popular tool used for UNIX-based systems and Pinger, and Ws PingPro Pack are used in Windows-based environments for performing Ping sweeps.
- Use the traceroute method to identify the paths from the Ping packets to the destination target. The routes can then be traced to the destination live hosts, detected using the Ping sweeps to derive an

estimated map of the organisation's architecture topology. The two commonly used tools are tracer route and tracert, available for both UNIX- and Windows-based operating systems. The purpose of this method is to identify the common and uncommon "hops" prior to reaching the destination targets, which could represent such things as firewalls, filtering routers or other gateways, load-balancing devices ,or web redirectors. It is not uncommon for network segments to have multiple connections to the Internet—unknown to the network group. However, these uncommon paths can lead to network compromises, if uncontrolled.

  - Send "bogus" e-mail messages to domains owned by the organisation in an attempt to receive a returned e-mail. Review the header of returned e-mails to determine possible network paths.

- To perform a vulnerability analysis:
  - Assess possible methods of attacks based on identification of vulnerabilities. To do this, identified machines within the target network are examined to identify all open ports, the operating systems (OS), the applications and their hosts (including version number, patch level and/or service pack). In addition, this information is compared with Internet vulnerability databases to ascertain what current vulnerabilities and exploits may be applicable to the target network.
  - Identify the type of OS employed by target hosts. For those target hosts identified in the network enumeration phase, the NMAP tool can be used to identify the type of OS employed. The type of OS employed is critical in predicting the types of service available and then to tailor the targeted analysis of service rendered through that port, which, when executed, will determine if specific vulnerabilities exist. In conjunction with this step is the need to obtain a current list of vulnerabilities for the OS employed by searching the OS vendor's

web site and vulnerability databases to obtain details of these vulnerabilities.

- Obtain permission to execute a port scan for those destination target hosts that are "live." A port scan may be needed on all possible ports (1-65535), if the security group is aware of the penetration testing. The list of ports should include applications that have known vulnerabilities. Ports examined should relate to weaknesses, vulnerabilities or information gathering. For example, the ports for file transfer protocol (FTP), Telnet, and RealSecure (ports 21, 23 and 2998) are often selected to attempt to exploit vulnerabilities. NMAP is the standard tool and can be programmed to execute a port scan for those destination target hosts that are "live" (from a port scan). Port scanning is clearly unethical without the express permission of the port owner. Port scanning, as with many other vulnerability tests, is a technique that may be employed by hackers, and should alarm the security group of a potential attempted penetration.
- Perform an application enumeration to identify assigned services (applications) of ports. In addition to the port scan, the specific identification of assigned services (applications) to a port is known as application enumeration. Knowing which applications the target hosts are running goes a long way toward performing a vulnerability analysis. Ordinarily, the applications are run through the Internet. Find a list of known vulnerabilities and exploits for these applications, which often comes from the vendors themselves and vulnerability databases. Application enumeration also involves banner grabbing, which may be helpful in identifying running applications. This can be done with many applications, including Netcat, which runs from either the UNIX or Windows command line; Telnet; and What's Running, a Windows GUI tool. Examples

	of common sources of information about system and application software vulnerabilities and exploits are Bugtraq lists, Packetstorm and SecurityFocus. o Run commercial or open source network vulnerability assessment tools to verify results. Popular tools include Nessus, ISS Internet Scanner, Foundstone's FoundScan, eEye's Retina Scanner and GFI's LANguard. • Exploit vulnerabilities identified in the vulnerability analysis to attempt to gain root or administrator-level access to the target systems or other trusted user account access as follows: o Document all relevant information upon access to the command line of a targeted system, via the access points identified in the vulnerability analysis, including the host and directory or share name to which access was gained; the host from which access was gained; date, time and the level of access; and finally the security hole(s) that were exploited to gain access. o Launch attacks against other systems on the network from the host that was compromised. If possible, a tool kit is installed on the exploited hosts that are tailored to the operating system of the other targeted machines to ascertain their vulnerabilities. The tool kit may include Netcat, password crackers, remote control software, sniffers and discovery tools, which can be executed from the command line. At this point, the method of Internet (external) penetration merges with internal testing methods described in section 5. o Notify the organisation if the access level is achieved, allowing installation of critical viruses that could result in consequential system outage.	
Dial-in Penetrati	• Gain penetration by dialing in over the telephone line that is listening for incoming connections, and log into the host machine. Example of	

on Testing	vulnerabilities searched for may include: o Modems attached to machines, such as routers, that are used by the hardware and software vendors to maintain it (i.e., installation of patches) o Rogue modems that are connected to actively listening users' desktops o Modems where remote management tools are installed, such as PCAnywhere o Modems that are authorised but insecurely configured • Gather the groupings of phone numbers used to make calls. Sources include phone books, online directories, company brochures and literature. Internal telephone directories may be particularly valuable, if accessible. These may be based on block(s) of phone numbers within a specified range that may be geographically assigned: o Find where the target organisation physically resides, which will define its area code and, to a lesser extent, its prefix. o Attempt to obtain these numbers independently of the organisation to ascertain the difficulty. It may require a level of social engineering. • Identify listening modems by calling each number in the target range randomly. War dialing software can be employed to dial and record the responses to determine if there is a modem listening. • After detecting a modem that is listening, gain unauthorised access by making brute force default passwords or strategic guessing attempts on the username/password challenge. War dialing software can be set to attempt to gain login access by using the largest list possible and/or selective list of default user IDs and passwords. The selective default list may also include strategic guesses of the user ID/password pair. For example, for a Cisco router, the username/password pair may be Cisco/Cisco or enable/Cisco or, when only a password is asked c, cc, cisco, and Cisco router, may be	

	attempted. Vendor provided default user ID/password pairs should be attempted, as these are very often not changed or disabled. • Determine whether sniffers and keyboard loggers are installed on web devices within the demilitarised zone (DMZ) to pick up user IDs and passwords. • Consider whether PCAnywhere is being used, configured to allow connection without authentication as long as the calling client is using the PCAnywhere.	
Internal Penetration Testing	• Perform a network discovery test using the following steps: o Perform a Ping sweep to identify live hosts. Popular tools include NMAP Pinger, NetScan tools and WS_Ping ProPack tools. o Also, if possible, install sniffers on the hosts that have been compromised in the external penetration test that identifies ARP tables, SNMP data and routing information. o Attempt to perform a zone transfer to learn internal IP addresses and computer names, which may indicate the purpose of the host. o Attempt to perform a tracer route to fine tune the target list of hosts deemed critical. o Guess the community strings or whether it was set to public or private to obtain SNMP information, which includes routing tables, protocols, error logs, and other system and network data, to build an attack. Also attempt to guess commonly used community strings (e.g., Cisco, {company name}, router, switch, network) o After completing the above, obtain authorisation from the security group to install host-based automated discovery tools that provide a full listing of vulnerabilities. Popular tools include Enterprise Security Manager (ESM), ISS, etc. • Perform a vulnerability analysis using the following steps: o Execute a port scan and banner grabbing programs on the target	

hosts to identify active services. This is comparable to external penetration testing. This step can be performed in conjunction with the Ping sweeps using NMAP.

- Test the individual known vulnerabilities for each type of system software, in conjunction with the open ports for exploitation. For example, known anonymous FTP vulnerabilities should be tested to determine if these weaknesses could be exploited by utilising an exploit script and subsequently installing a root kit containing Netcat to open up a command prompt on a particular point. There are numerous known vulnerabilities that constantly expand.
- Obtain authorisation from the security group to install automated discovery tools that provide a full listing of vulnerabilities. These tools include CyperCop, Enterprise Security Manager (ESM) and Internet Security Scanner (ISS) and Nessus.
- Generate a schedule of IP addresses host names, types of system software (i.e., UNIX and NT), open ports and application (Netscape and IIS and Apache).

- Perform the exploitation and notification using the following steps:
  - Determine the level of attack that the organisation would desire and approve.
  - Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by the organisation. For example, if the target host is UNIX-based, the next step after gaining access to this device could be to attempt to crack the password file. In addition, if the attacker can obtain access to other devices and valuable organisation data without detection, the penetration was a full success.
  - Notify the organisation if access level is achieved, allowing installation of critical viruses or root kits or other tools or software

	that could result in consequential system outage or to demonstrate the ability of an attacker to retain unauthorised access devoid of detection. o Record all vulnerabilities noted and provide to the organisation for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.	
Physical Access Controls	• Search for rogue access jacks that can be exploited. Identify telecommunication access paths into and out of the business and data centre area. Access paths should be buried or cancelled and not accessible by the general public. Attempt to identify cabling in ceilings or closets where an unauthorised tap can occur, though this may not be always possible especially given the use of fiber optic cable. • Perform brute and selective access to default user IDs once access to the network is physically obtained. • Obtain physical access and initiate social engineering as defined in section 7 of this procedure: o Without authentication as an employee one should attempt to obtain unimpeded access. For those organisation sites with physical security via mechanical, electronic or physical guard, this testing can be accomplished in multiple ways including piggybacking into the site with a legitimate employee or signing in without an escort and walking directly into the data centre or business work sites. o Standard business practice should restrict direct unimpeded access to all work areas. o The consulting agreement or internal auditor performing the test should explicitly require this evaluation. o A data centre audit should be performed to evaluate all the physical controls to the data centre and other work sites. • Create burs around the data centre complex to avoid intruders or interlopers	

	from obtaining transmission signals.	
Social Engineering Testing	• Test controls to prevent social engineering or circumvention of logical security measure in place by masquerading as an individual calling over an internal phone with a business need requesting critically sensitive information or access to basic computing services. • Explicitly allow he penetration testing contract, if performed by external consultants, to test garbage disposal areas. • Review confidentially polices and practices to ascertain whose responsibility it is for the disposing and shredding of organisation-related information in hard copy form. • Safeguards for the disposal of data are critical. • Review measures for the disposal of magnetic media holding sensitive data. • Review individual employee work areas as well as printer baskets for propriety information, such as user ID, other employee's information and computer names, if physical access to the work area is obtained. Sticky notes and to-do lists can be sources of important information. • Obtain a building and floor schematic of critical areas. Work areas, such as the treasury and disbursement departments as well as executive offices, are primary targets. • Determine whether individual desktop computers have a screen saver and work desks are locked. Provide reasonable assurance the scope of the work does not break any laws.	
Wireless	• Find and map the wireless networks into a street or physical geographic area map. The tools needed to perform a penetration test of a wireless network may include a laptop/PDA, a wireless NIC (ORiNOCO or Lucent PC, Card Dell TrueMobile 1150, Avaya Wireless PC Card, Compaq WL110, Enterasys Roamabout Elsa Airlancer MC-11), freeware software, and an antenna and GPS. One technique used for finding a wireless network is War Driving. This is done by detecting the beacon and broadcast. War Driving is	

	used to capture and map wireless band signal. • Crack the WEP (Wired Equivalent Privacy) keys by using automated tools such as WEPCrack and AirSnort. The techniques used include IV Collisions and Weak key packet capture. • Sniff and analyse the network traffic to ascertain the number of packet passes, SSID, etc. There are a variety of automated tools, such as PrismDump, Iris, AiroPeek and Sniffer Wireless. • After the key is known, reassemble the packet to complete the penetration test. Document all issues noted for management review. Before this test, it is best to consult legal representatives practicing within the individual countries and, where necessary, local and state municipalities to provide reasonable assurance that performing this test will not violate any laws or regulations due to picking up information packets from other unintended targets.	
Web Application	• Analyse the web application and environment by first crawling through the web pages to gather the information including mapping of all pages and general understanding of all functionality to ascertain risk. Specifically, manually surf the application with a recording proxy (e.g., webproxy, ebsleuth) to find hidden data and locate form weaknesses. In conjunction with this survey, complete the following: o Review inventory SSL/TLS ciphers to determine accordance with policies or standard industry practices. o Analyse session tracking including mechanism and session ID. o Identify authentication methods employed, including client certificates, auditing and revoking certificates, use of encryption or HTTP basic authentication and deployment of SSL. o Identify sign-on and sign-off (use of anticaching techniques and session inactivity cause automatic sign-off) mechanisms. o Identify all points of user input by recording every form element,	

specifically:

- Test SQL injection
- Attempt buffer overflow to gain control
- Cross-site scripting (XSS)
- Special characters (pipes, returns, etc.)
- For numeric input try 0, a negative value, a really large value

o Record any verbose error messages. In addition, test any HTTP headers being used as input such as:

- Cookie, Referrer, Host, User-agent
- Record permutation list used
- Record any verbose error messages
- Test user input embedded into URL for POST

o Review for hidden content or information leakage in Web Application Output

- Search for client-side code for unnecessary information (meta tags, comments).
- Ascertain if HTTP from server for unneeded information (Server:, X-).
- Determine if Java applets and similar are decompiled.
- Retrieve robots.txt file for each known directory and review.

o Review security over session IDs including the following tests:

- Determine if they are random, not related to user information, large enough to avoid brute force, perishable, transmitted over secured path, controls to prevent tempering, and have a detection mechanism.
- Determine that cookies with session IDs are marked “secure” (encrypted), nonpersistent (not stored on hard-drive), reasonably limited to path and domain and, if appropriate, digitally signed.
- Verify URLs with session ID are sent with encryption, such as SSL.

- Review controls over sign-on including the:
  - Warning banner and error messages to warn against an unauthorised hacking attempt
  - Generic message does not providing specific knowledge of which is incorrect when a login is made with an invalid password or login account
  - Encryption of initial login involving credentials
  - Timeout after a period of inactivity to prevent half open sessions
  - Lockout mechanism for invalid login attempts to minimise exposure to brute-force attacks
  - Lock mechanism does not result in denial of service of a substantial number of suspended login accounts, rather it provides notification of attack resulting in an escalation process
- Determine if all information transmitted is encrypted, such as verifying lock is shown on web browser. Ascertain if all pages sent and received are encrypted.

- Collectively review results of the survey evaluation and results of the portal testing steps to ascertain the vulnerabilities that could be exploited to gain access to sensitive information by an outsider with no information of the system and no login account andan insider with knowledge of the system with a login account.

Note: Since there are significant numbers of exploits detected via port 80, as time goes by, it is recommended that those performing this test possess current knowledge that would exceed that which is defined in various research documents, white pages and web sites. In addition, there is a series of audit testing of the web servers, including standard access control list evaluation and TCP/IP weakness, that should be performed and are included in other sections of this procedure.

- Run commercial or open source application vulnerability assessment tools to verify results. Popular tools include Nikto, WebInspect, ScanDo and

	Appscan. • There are numerous potential vulnerabilities that could be detected by performing the above testing. Accordingly, the second step is to exploit potential vulnerabilities, which would include, but are not limited to, the following: o Alter contents of cookies (e.g., altering the parameters passed to the application through a URL) resulting in access to sensitive information or impersonating another user. o Change JavaScript within the application or hidden form files on application forms, parameter tampering, SQL injection (passing SQL code into an application that was not intended), cross-site scripting (entering executable commands into web site buffers). o Insert code into text fields to take control of an application. o Directly access a web page that can ordinarily only be reached through authentication by a brute force attack. Collect user IDs where wrong passwords are entered and execute the dictionary against them. o Directly exploit backdoors and debug options including executing debug syntax on URLs (e.g., there is a listing of vulnerabilities on various web sites including CERT and vendor sites, such as www.nstalker.com). o Exploit any configuration errors in third-party applications, such as web or database servers. Specific attempts should be made to exploit web server default configuration vulnerabilities that are known. o Insert scripting languages in a text field that other users will see. o Pass excessive data in an application request (e.g., sending large numbers of characters to a web site form/field).	
Report	• Prepare report in accordance with ISACA IS Auditing Standards including: o Defining the scope	

	○ Objectives ○ Period of work performed ○ Nature, timing and extent of the penetration testing and vulnerability analysis performed ○ Conclusion as to the effectiveness of controls and the significance of vulnerabilities identified • Follow-up to provide reasonable assurance that controls were implemented and security holes were plugged on all known vulnerabilities. • Perform a specific process and attribute review of perimeter firewalls and routers, and discuss risks identified with management.	

CÓDIGO APLICACIÓN

En este apartado se muestra el código empleado para la realización del cuestionario. Está hecho en Delphi, se ha usado este lenguaje porque permite hacer un entorno gráfico adecuado a lo que se estaba buscando, además de esto ofrece la posibilidad de pasar los datos finales a gráficas permitiendo de esta manera que el usuario vea de una manera más clara y global como ha quedado en cuestión la auditoría.

Primeramente se muestran las unidades usadas y al final el programa principal para que se lance la aplicación.

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls;

type
  TPantalla1 = class(TForm)
    b: TLabel;
    Label1: TLabel;
    Button1: TButton;
    Button2: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla1: TPantalla1;

implementation

{$R *.dfm}

USES
   Unit2;
```

```
procedure TPantalla1.Button1Click(Sender: TObject);
begin
   Pantalla2.Visible:= True;
   Pantalla1.Visible:= False;

end;

procedure TPantalla1.Button2Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit2;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit1;

type
  TPantalla2 = class(TForm)
    Label1: TLabel;
    RadioGroup1: TRadioGroup;
    Label2: TLabel;
    RadioGroup2: TRadioGroup;
    Button1: TButton;
    Label3: TLabel;
    RadioGroup3: TRadioGroup;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);

  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
    FUNCTION Media: Double;

  end;


var
  Pantalla2: TPantalla2;


implementation

USES unit3, Unit18;

CONST
   Bloque= 1;
   MaxBloques=5;
   MaxPreguntas=3;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);
```

```
VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;

{$R *.dfm}


FUNCTION TPantalla2.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla2.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla2.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;


FUNCTION TPantalla2.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total;
END;

FUNCTION TPantalla2.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total;
END;
```

```
FUNCTION TPantalla2.Media: Double;

VAR max: Integer;
    min: Integer;


BEGIN
    min:= Pantalla2.GetMin;
    max:= Pantalla2.GetMax;

    Media:= (min+max)/2;


END;

procedure TPantalla2.Button1Click(Sender: TObject);
begin

   IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) OR
(RadioGroup3.ItemIndex = -1) THEN
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup1.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup2.ItemIndex+1];
   Resultado[3]:= Ponderacion[3]*Puntuacion[RadioGroup3.ItemIndex+1];



   Pantalla3.Visible:= True;
   Pantalla2.Visible:= False;

   END;
end;

procedure TPantalla2.Button2Click(Sender: TObject);
begin

    Pantalla1.Visible:= True;
    Pantalla2.Visible:= False;

end;

procedure TPantalla2.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;

begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I);
end;

procedure TPantalla2.Button3Click(Sender: TObject);
```

```
begin
Application.Terminate;
end;

end.
```

```
unit Unit3;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, unit2;

type
  TPantalla3 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla3: TPantalla3;

implementation



{$R *.dfm}

USES Unit4;







procedure TPantalla3.Button1Click(Sender: TObject);
begin

    Pantalla4.Visible:= True;
    Pantalla3.Visible:= False;

end;



procedure TPantalla3.Button2Click(Sender: TObject);
begin

    Pantalla2.Visible:= True;
```

```
    Pantalla3.Visible:= False;

end;

procedure TPantalla3.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit4;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit3;

type
  TPantalla4 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    RadioGroup3: TRadioGroup;
    RadioGroup1: TRadioGroup;
    RadioGroup2: TRadioGroup;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);

  private
    { Private declarations }
  public
    { Public declarations }
     FUNCTION GetBloque: Integer;
     FUNCTION GetMaxPreguntas: Integer;
     FUNCTION Evaluate: Integer;
     FUNCTION GetMax: Integer;
     FUNCTION GetMin: Integer;
     FUNCTION Media: Double;
  end;

var
  Pantalla4: TPantalla4;


implementation

USES Unit5, Unit18;

CONST
   Bloque= 2;
   MaxBloques= 5;
   MaxPreguntas=3;
   MaxPuntos=5;

   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;
```

```
{$R *.dfm}

FUNCTION TPantalla4.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla4.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla4.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla4.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total;
END;

FUNCTION TPantalla4.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total;
END;

FUNCTION TPantalla4.Media: Double;

VAR max: Integer;
    min: Integer;
```

```
BEGIN
    min:= Pantalla4.GetMin;
    max:= Pantalla4.GetMax;

    Media:= (min+max)/2;



END;

procedure TPantalla4.Button1Click(Sender: TObject);
begin
  IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) OR
(RadioGroup3.ItemIndex = -1) THEN
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup1.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup2.ItemIndex+1];
   Resultado[3]:= Ponderacion[3]*Puntuacion[RadioGroup3.ItemIndex+1];


   Pantalla5.Visible:= True;
   Pantalla4.Visible:= False;

   END;
END;



procedure TPantalla4.Button2Click(Sender: TObject);
begin

    Pantalla3.Visible:= True;
    Pantalla4.Visible:= False;

end;

procedure TPantalla4.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;


begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+3);
end;


procedure TPantalla4.Button3Click(Sender: TObject);
begin
```

```
Application.Terminate;
end;

end.
```

```
unit Unit5;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, unit4;

type
  TPantalla5 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla5: TPantalla5;

implementation


{$R *.dfm}

USES Unit6;



procedure TPantalla5.Button1Click(Sender: TObject);
begin

    Pantalla6.Visible:= True;
    Pantalla5.Visible:= False;


end;

procedure TPantalla5.Button2Click(Sender: TObject);
begin
      Pantalla4.Visible:= True;
      Pantalla5.Visible:= False;

end;

procedure TPantalla5.Button3Click(Sender: TObject);
```

```
begin
Application.Terminate;
end;

end.
```

```
unit Unit6;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit5;

type
  TPantalla6 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    RadioGroup2: TRadioGroup;
    RadioGroup3: TRadioGroup;
    RadioGroup1: TRadioGroup;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
  end;

var
  Pantalla6: TPantalla6;

implementation

USES Unit7, Unit18;

CONST
   Bloque=3;
   MaxBloques= 5;
   MaxPreguntas=3;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;

{$R *.dfm}
```

```
FUNCTION TPantalla6.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla6.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla6.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla6.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total;
END;

FUNCTION TPantalla6.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total;
END;


procedure TPantalla6.Button1Click(Sender: TObject);
begin

   IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) OR
(RadioGroup3.ItemIndex = -1) THEN
```

```
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup1.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup2.ItemIndex+1];
   Resultado[3]:= Ponderacion[3]*Puntuacion[RadioGroup3.ItemIndex+1];



   Pantalla7.Visible:= True;
   Pantalla6.Visible:= False;

   END;

end;


procedure TPantalla6.Button2Click(Sender: TObject);
begin
   Pantalla5.Visible:= True;
   Pantalla6.Visible:= False;

end;

procedure TPantalla6.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;


begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+6);
end;



procedure TPantalla6.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit7;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit6;

type
  Tpantalla7 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    RadioGroup1: TRadioGroup;
    RadioGroup3: TRadioGroup;
    Button1: TButton;
    Label3: TLabel;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
    FUNCTION Media: Double;
    FUNCTION GetMinSubB: Integer;
    FUNCTION GetMaxSubB: Integer;
  end;

var
  pantalla7: Tpantalla7;

implementation

USES Unit8, Unit10, Unit18;

CONST
   Bloque=3;
   MaxBloques= 5;
   MaxPreguntas=2;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;
```

```
{$R *.dfm}


FUNCTION TPantalla7.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla7.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla7.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla7.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total + Pantalla6.GetMax;
END;

FUNCTION TPantalla7.GetMaxSubB: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMaxSubB:= Total;
END;


FUNCTION TPantalla7.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
```

```
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total + Pantalla6.GetMin;

END;

FUNCTION TPantalla7.GetMinSubB: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMinSubB:= Total;

END;

FUNCTION TPantalla7.Media: Double;

VAR max: Integer;
    min: Integer;


BEGIN
    min:= Pantalla7.GetMin;
    max:= Pantalla7.GetMax;

    Media:= (min+max)/4;



END;

procedure TPantalla7.Button1Click (Sender: TObject);
begin

   IF (RadioGroup3.ItemIndex = -1) OR (RadioGroup1.ItemIndex = -1){* OR
(RadioGroup3.ItemIndex = -1) *} THEN

      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup3.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup1.ItemIndex+1];
    Pantalla8.Visible:= True;
    Pantalla7.Visible:= False;

   END;
end;
```

```
procedure Tpantalla7.Button2Click(Sender: TObject);
begin

     Pantalla6.Visible:= True;
     Pantalla7.Visible:= False;

end;

procedure Tpantalla7.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;

begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+9);
end;



procedure Tpantalla7.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit8;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, unit7;

type
  TPantalla8 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla8: TPantalla8;

implementation

USES Unit9;


{$R *.dfm}




procedure TPantalla8.Button1Click(Sender: TObject);
begin

   Pantalla9.Visible:= True;
   Pantalla8.Visible:= False;

end;


procedure TPantalla8.Button2Click(Sender: TObject);
begin

    Pantalla7.Visible:= True;
    Pantalla8.Visible:= False;

end;

procedure TPantalla8.Button3Click(Sender: TObject);
```

```
begin
Application.Terminate;
end;

end.
```

```
unit Unit9;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit8;

type
  TPantalla9 = class(TForm)
    Button1: TButton;
    Label6: TLabel;
    RadioGroup1: TRadioGroup;
    RadioGroup2: TRadioGroup;
    Label1: TLabel;
    Label2: TLabel;
    Label7: TLabel;
    RadioGroup4: TRadioGroup;
    RadioGroup5: TRadioGroup;
    Label3: TLabel;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
  end;

var
  Pantalla9: TPantalla9;

implementation

USES Unit10, Unit18;

CONST
   Bloque=4;
   MaxBloques= 5;
   MaxPreguntas=4;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;
```

```
{$R *.dfm}

FUNCTION TPantalla9.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla9.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla9.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla9.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total;
END;

FUNCTION TPantalla9.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total;
END;

procedure TPantalla9.Button1Click(Sender: TObject);
begin

   IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) OR
(RadioGroup5.ItemIndex = -1) OR (RadioGroup4.ItemIndex = -1)THEN
```

```
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup4.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup5.ItemIndex+1];
   Resultado[3]:= Ponderacion[3]*Puntuacion[RadioGroup1.ItemIndex+1];
   Resultado[4]:= Ponderacion[4]*Puntuacion[RadioGroup2.ItemIndex+1];

        Pantalla10.Visible:= True;
        Pantalla9.Visible:= False;


   END;

end;


procedure TPantalla9.Button2Click(Sender: TObject);
begin

    Pantalla8.Visible:= True;
    Pantalla9.Visible:= False;

    end;


procedure TPantalla9.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;

begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+11);
end;



procedure TPantalla9.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit10;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit9;

type
  TPantalla10 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    RadioGroup3: TRadioGroup;
    RadioGroup1: TRadioGroup;
    RadioGroup2: TRadioGroup;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
    FUNCTION Media: Double;
  end;

var
  Pantalla10: TPantalla10;

implementation

USES Unit11, Unit18;

CONST
   Bloque=4;
   MaxBloques= 5;
   MaxPreguntas=3;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;
```

```
{$R *.dfm}

FUNCTION TPantalla10.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla10.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla10.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla10.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total + Pantalla9.GetMax;
END;

FUNCTION TPantalla10.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total + Pantalla9.GetMin;
END;

FUNCTION TPantalla10.Media: Double;

VAR max: Integer;
    min: Integer;

BEGIN
```

```
    min:= Pantalla10.GetMin;
    max:= Pantalla10.GetMax;

   Media:= (min+max)/4;
END;

procedure TPantalla10.Button1Click(Sender: TObject);
begin

   IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) OR
(RadioGroup3.ItemIndex = -1) THEN
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup1.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup2.ItemIndex+1];
   Resultado[3]:= Ponderacion[3]*Puntuacion[RadioGroup3.ItemIndex+1];


     Pantalla11.Visible:= True;
     Pantalla10.Visible:= False;
   END;

end;



procedure TPantalla10.Button2Click(Sender: TObject);
begin
     Pantalla9.Visible:= True;
     Pantalla10.Visible:= False;
end;

procedure TPantalla10.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;


begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+15);
end;


procedure TPantalla10.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit11;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit10;

type
  TPantalla11 = class(TForm)
    RadioGroup2: TRadioGroup;
    RadioGroup3: TRadioGroup;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
    FUNCTION Media: Double;
    FUNCTION GetMinSubB: Integer;
    FUNCTION GetMaxSubB: Integer;
  end;

var
  Pantalla11: TPantalla11;

implementation

USES Unit12, Unit18;

CONST
   Bloque=4;
   MaxBloques= 5;
   MaxPreguntas=2;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;
```

```
{$R *.dfm}


FUNCTION TPantalla11.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla11.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla11.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla11.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total + Pantalla10.GetMax;
END;

FUNCTION TPantalla11.GetMaxSubB: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMaxSubB:= Total;
END;


FUNCTION TPantalla11.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
```

```
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total + Pantalla10.GetMin;
END;

FUNCTION TPantalla11.GetMinSubB: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMinSubB:= Total;
END;


FUNCTION TPantalla11.Media: Double;

VAR max: Integer;
    min: Integer;


BEGIN
    min:= Pantalla11.GetMin;
    max:= Pantalla11.GetMax;

    Media:= (min+max)/4;

END;

procedure TPantalla11.Button1Click(Sender: TObject);
begin

   IF (RadioGroup3.ItemIndex = -1) OR (RadioGroup2.ItemIndex = -1) {*OR
(RadioGroup3.ItemIndex = -1) *} THEN

      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup3.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup2.ItemIndex+1];



   Pantalla12.Visible:= True;
   Pantalla11.Visible:= False;

   END;
end;
```

```
procedure TPantalla11.Button2Click(Sender: TObject);
begin

   Pantalla10.Visible:= True;
   Pantalla11.Visible:= False;

end;

procedure TPantalla11.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;


begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+18);
end;



procedure TPantalla11.Button3Click(Sender: TObject);
begin
Application.Terminate;
end;

end.
```

```
unit Unit12;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, unit11;

type
  TPantalla12 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla12: TPantalla12;

implementation

USES Unit13;


{$R *.dfm}




procedure TPantalla12.Button1Click(Sender: TObject);
begin

     Pantalla13.Visible:= True;
     Pantalla12.Visible:= False;
end;


procedure TPantalla12.Button2Click(Sender: TObject);
begin

    Pantalla11.Visible:= True;
    Pantalla12.Visible:= False;
end;

procedure TPantalla12.Button3Click(Sender: TObject);
```

```
begin
Application.Terminate;
end;

end.
```

```
unit Unit13;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, unit12;

type
  TPantalla13 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    RadioGroup1: TRadioGroup;
    Button1: TButton;
    RadioGroup3: TRadioGroup;
    Button2: TButton;
    Button3: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }

    FUNCTION GetBloque: Integer;
    FUNCTION GetMaxPreguntas: Integer;
    FUNCTION Evaluate: Integer;
    FUNCTION GetMax: Integer;
    FUNCTION GetMin: Integer;
    FUNCTION Media: Double;

  end;

var
  Pantalla13: TPantalla13;

implementation

USES unit14, Unit18;

CONST
   Bloque=5;
   MaxBloques= 5;
   MaxPreguntas=2;
   MaxPuntos=5;
   Puntuacion: ARRAY [1..MaxPuntos] OF Integer = (1,2,3,4,5);

VAR
   Resultado: ARRAY[1..MaxPreguntas] OF Integer;
   Ponderacion: ARRAY[1..MaxPreguntas] OF Integer;

{$R *.dfm}
```

```
FUNCTION TPantalla13.GetBloque: Integer;
BEGIN
   GetBloque:= Bloque;
END;


FUNCTION TPantalla13.GetMaxPreguntas: Integer;
BEGIN
   GetMaxPreguntas:= MaxPreguntas
END;

// FUNCION QUE SUMA LOS VALORES DE LAS RESPUESTAS

FUNCTION TPantalla13.Evaluate: Integer;
VAR
   I: 1..MaxPreguntas;
   Total: Integer;

BEGIN
   Total:= 0;
   FOR I:=1 TO MaxPreguntas DO
      Total:= Total+Resultado[I];

   Evaluate:= Total;
END;

FUNCTION TPantalla13.GetMax: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[MaxPuntos];

    GetMax:= Total;
END;

FUNCTION TPantalla13.GetMin: Integer;
VAR
   I, Total: Integer;
BEGIN
    Total:= 0;
    FOR I:= 1 TO MaxPreguntas DO
       Total:= Total+Ponderacion[I]*Puntuacion[1];

    GetMin:= Total;
END;

FUNCTION TPantalla13.Media: Double;

VAR max: Integer;
    min: Integer;


BEGIN
    min:= Pantalla13.GetMin;
```

```
    max:= Pantalla13.GetMax;

    Media:= (min+max)/2;



END;

procedure TPantalla13.Button1Click(Sender: TObject);
begin

   IF (RadioGroup1.ItemIndex = -1) OR (RadioGroup3.ItemIndex = -1) {*OR
(RadioGroup3.ItemIndex = -1) *} THEN
      Application.MessageBox('Falta alguna pregunta por puntuar',
'Error', mb_OK)
   ELSE
      BEGIN


   Resultado[1]:= Ponderacion[1]*Puntuacion[RadioGroup3.ItemIndex+1];
   Resultado[2]:= Ponderacion[2]*Puntuacion[RadioGroup1.ItemIndex+1];


        Pantalla14.Visible:= True;
        Pantalla13.Visible:= False;
   END;
end;




procedure TPantalla13.Button2Click(Sender: TObject);
begin

    Pantalla12.Visible:= True;
    Pantalla13.Visible:= False;
end;



procedure TPantalla13.FormShow(Sender: TObject);
VAR
   I: 1..MaxPreguntas;


begin
   FOR I:= 1 TO MaxPreguntas DO
      Ponderacion[i]:= Pantalla18.PesoPregunta(I+20);
end;


procedure TPantalla13.Button3Click(Sender: TObject);
begin
Application.Terminate;
```

```
end;
end.
```

```
unit Unit14;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, unit15;

type
  TPantalla14 = class(TForm)
    Button1: TButton;
    Button2: TButton;
    procedure Button2Click(Sender: TObject);
    procedure Button1Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla14: TPantalla14;

implementation

{$R *.dfm}

USES Unit16;

procedure TPantalla14.Button2Click(Sender: TObject);
begin

    Pantalla15.Visible:= True;
    Pantalla14.Visible:= False;
end;

procedure TPantalla14.Button1Click(Sender: TObject);
begin
   Pantalla14.Hide;
   Pantalla16.Show;

end;

end.
```

```
unit Unit15;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, TeeProcs, TeEngine, Chart, Buttons, jpeg;

type
  TPantalla15 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Label5: TLabel;
    Label6: TLabel;
    Label7: TLabel;
    Label8: TLabel;
    Label9: TLabel;
    Label10: TLabel;
    BitBtn1: TBitBtn;
    BitBtn2: TBitBtn;
    Button1: TButton;
    Label11: TLabel;
    Label12: TLabel;
    Label13: TLabel;
    Label14: TLabel;
    Label15: TLabel;
    Label16: TLabel;
    Label17: TLabel;
    Label18: TLabel;
    Label19: TLabel;
    FELIZ: TImage;
    SERIO: TImage;
    Image1: TImage;
    Image2: TImage;
    Image3: TImage;
    Image4: TImage;
    Image5: TImage;
    Image6: TImage;
    Image7: TImage;
    Image8: TImage;
    Image9: TImage;
    Image10: TImage;
    Image11: TImage;
    Image12: TImage;
    Image13: TImage;
    Image14: TImage;
    Image15: TImage;
    Image16: TImage;
    procedure BitBtn2Click(Sender: TObject);
    procedure BitBtn1Click(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
  private
```

```
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla15: TPantalla15;

implementation

{$R *.dfm}
USES Unit2, Unit4, Unit6, Unit7, Unit9, Unit10, Unit11, Unit13, Unit14,
  Unit17, Unit16;

procedure TPantalla15.BitBtn2Click(Sender: TObject);
begin

Pantalla17.Visible:=True;
Pantalla15.Visible:=False;

end;

procedure TPantalla15.BitBtn1Click(Sender: TObject);
begin

Pantalla16.Visible:=True;
Pantalla15.Visible:=False;
end;

procedure TPantalla15.Button1Click(Sender: TObject);
begin

Application.Terminate;
end;



procedure TPantalla15.FormShow(Sender: TObject);

CONST
   Pantallas=2;
   MaxBloques=5;
   MaxPreguntasBloqueI= 3;
   MaxPreguntasBloqueII=3;
   MaxPreguntasBloqueIII1=3;
   MaxPreguntasBloqueIII2=2;
   MaxPreguntasBloqueIII=5;
   MaxPreguntasBloqueIV1=4;
   MaxPreguntasBloqueIV2=3;
   MaxPreguntasBloqueIV=2;
   MaxPreguntasBloqueV=2;
VAR
```

```
   MediaBloqueIII: Double;

   MediaBloqueIV: Double;


  // min, max : integer;


begin
  { SumaTotal:=0;
   SumaTotal:= Pantalla2.Evaluate;
   SumaTotal:= SumaTotal+Pantalla4.Evaluate;
   SumaTotal:= SumaTotal+Pantalla6.Evaluate;
   SumaTotal:= SumaTotal+Pantalla7.Evaluate;
   SumaTotal:= SumaTotal+Pantalla9.Evaluate;
   SumaTotal:= SumaTotal+Pantalla10.Evaluate;
   SumaTotal:= SumaTotal+Pantalla11.Evaluate;
   SumaTotal:= SumaTotal+Pantalla13.Evaluate;

 }


   MediaBloqueIII:=(Pantalla6.Evaluate+Pantalla7.Evaluate)/2;
   MediaBloqueIV:=(Pantalla9.Evaluate + Pantalla10.Evaluate +
Pantalla11.Evaluate)/2;



    IF (Pantalla2.Evaluate >= Pantalla2.Media) THEN
         BEGIN
ES UN: ' +  strAux;
            Label11.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
BLOQUE';
            Image1.Visible:=True;
         END
    ELSE
         BEGIN
            Label11.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE BLOQUE';
            Image2.Visible:=True;
         END;



    IF Pantalla4.Evaluate >= Pantalla4.Media THEN
         BEGIN
            Label12.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
BLOQUE';
            Image3.Visible:=True;
         END
    ELSE
         BEGIN
            Label12.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE BLOQUE';
```

```
            Image4.Visible:=True;
         END;



   IF MediaBloqueIII  >= Pantalla7.Media THEN
         BEGIN

            Label13.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
BLOQUE';
            FELIZ.Visible:=True;
         END
    ELSE
         BEGIN
             Label13.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE BLOQUE';
            SERIO.Visible:=True;
         END;


   IF Pantalla6.Evaluate  >= ((Pantalla6.GetMin + Pantalla6.GetMax)/2)
THEN
         BEGIN
             Label14.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
SUB_BLOQUE';
            Image5.Visible:=True;
         END
    ELSE
         BEGIN

            Label14.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE SUB_BLOQUE';
            Image6.Visible:=True;
         END;


   IF Pantalla7.Evaluate  >= ((Pantalla7.GetMinSubB +
Pantalla7.GetMaxSubB)/2) THEN
         BEGIN

            Label15.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
SUB_BLOQUE';
            Image7.Visible:=True;
         END
    ELSE
         BEGIN
            Label15.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE SUB_BLOQUE';
            Image8.Visible:=True;
         END;



    IF MediaBloqueIV >= Pantalla11.Media THEN
         BEGIN
```

```
            Label16.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
BLOQUE';
            Image9.Visible:=True;
         END
    ELSE
         BEGIN
            Label16.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE BLOQUE';
            Image10.Visible:=True;
         END;


    IF (Pantalla9.Evaluate+Pantalla10.Evaluate)  >= Pantalla10.Media
THEN
         BEGIN

            Label17.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
SUB_BLOQUE';
            Image11.Visible:=True;
         END
    ELSE
         BEGIN

            Label17.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE SUB_BLOQUE';
            Image12.Visible:=True;
         END;

    IF Pantalla11.Evaluate  >=
((Pantalla11.GetMaxSubB+Pantalla11.GetMinSubB)/2) THEN
         BEGIN

            Label18.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
SUB_BLOQUE';
            Image13.Visible:=True;
         END
    ELSE
         BEGIN
            Label18.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE SUB_BLOQUE';
            Image14.Visible:=True;
         END;




    IF Pantalla13.Evaluate >= Pantalla13.Media THEN
         BEGIN
            Label19.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO EN ESTE
BLOQUE';
            Image15.Visible:=True;
         END
    ELSE
         BEGIN
```

```
            Label19.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO EN
ESTE BLOQUE';
            Image16.Visible:=True;
         END;




end;




end.
```

```
unit Unit16;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, jpeg, ExtCtrls;

type
  TPantalla16 = class(TForm)
    Button1: TButton;
    Button2: TButton;
    Label1: TLabel;
    Label2: TLabel;
    Button3: TButton;
    Label3: TLabel;
    Image1: TImage;
    Image2: TImage;
    Label4: TLabel;
    procedure FormShow(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);

  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla16: TPantalla16;

implementation

{$R *.dfm}
USES Unit2, Unit4, Unit6, Unit7, Unit9, Unit10, Unit11, Unit13, Unit15,
Unit17 ;


procedure TPantalla16.FormShow(Sender: TObject);
CONST
   Pantallas=2;
   MaxBloques=5;
   MaxPreguntasBloqueI= 3;
   MaxPreguntasBloqueII=3;
   MaxPreguntasBloqueIII1=3;
   MaxPreguntasBloqueIII2=2;
   MaxPreguntasBloqueIII=5;
   MaxPreguntasBloqueIV1=4;
   MaxPreguntasBloqueIV2=3;
   MaxPreguntasBloqueIV=2;
   MaxPreguntasBloqueV=2;
VAR
   Suma: double;
```

```
   StrAux: String;
   ResultadoFinal: Double;
   SumarMediasBloques: Double;
   MediaBloqueIII: Double;
   MediaBloqueIV: Double;


begin
  { SumaTotal:=0;
   SumaTotal:= Pantalla2.Evaluate;
   SumaTotal:= SumaTotal+Pantalla4.Evaluate;
   SumaTotal:= SumaTotal+Pantalla6.Evaluate;
   SumaTotal:= SumaTotal+Pantalla7.Evaluate;
   SumaTotal:= SumaTotal+Pantalla9.Evaluate;
   SumaTotal:= SumaTotal+Pantalla10.Evaluate;
   SumaTotal:= SumaTotal+Pantalla11.Evaluate;
   SumaTotal:= SumaTotal+Pantalla13.Evaluate;

 }


   MediaBloqueIII:=(Pantalla6.Evaluate+Pantalla7.Evaluate)/2;


   MediaBloqueIV:=(Pantalla9.Evaluate + Pantalla10.Evaluate +
Pantalla11.Evaluate)/2;


   SumarMediasBloques:= (Pantalla2.Evaluate + Pantalla4.Evaluate +
MediaBloqueIII + MediaBloqueIV + Pantalla13.Evaluate)/MaxBloques;
//Calcula la media obtenida con los resultados



  Suma:=Pantalla2.Media + Pantalla4.Media + Pantalla7.Media +
Pantalla11.Media + Pantalla13.Media;

  ResultadoFinal:=Suma/MaxBloques;   //Calcula la media mínima para
pasar la auditoría

  Str(SumarMediasBloques:2:2, StrAux);



    IF SumarMediasBloques >= ResultadoFinal THEN
         BEGIN
            IF ((Pantalla2.Evaluate < (Pantalla2.Media/2))
                OR (Pantalla4.Evaluate < (Pantalla4.Media/2))
                OR (MediaBloqueIII < (Pantalla7.Media/2))
                OR (MediaBloqueIV  < (Pantalla11.Media/2))
                OR (Pantalla13.Evaluate < (Pantalla13.Media/2))) THEN
                BEGIN
                  Label1.Caption:= 'EL RESULTADO OBTENIDO EN LA
AUDITORÍA ES UN: ' +  strAux;
                  Label3.Caption:= 'LA AUDITORÍA NO HA PASADO CON
ÉXITO';
```

```
                  Label4.Caption:= 'ALGÚN BLOQUE ESTÁ MUY DEFICIENTE';
                  Image1.Visible:=True;
                END
            ELSE
              BEGIN
              Label1.Caption:= 'EL RESULTADO OBTENIDO EN LA AUDITORÍA ES
UN: ' +  strAux;
              Label3.Caption:= 'LA AUDITORÍA HA PASADO CON ÉXITO';
              Label4.Caption:= '';
              Image2.Visible:=True;
              END;
         END
    ELSE
         BEGIN
            Label1.Caption:= 'EL RESULTADO OBTENIDO EN LA AUDITORÍA ES
UN: ' +  strAux;
            Label3.Caption:= 'LA AUDITORÍA NO HA PASADO CON ÉXITO';
            Label4.Caption:='';
            Image1.Visible:=True;
         END;


end;

procedure TPantalla16.Button1Click(Sender: TObject);
begin

Pantalla15.Visible:=True;
Pantalla16.Visible:=False;

end;

procedure TPantalla16.Button2Click(Sender: TObject);
begin

Pantalla17.Visible:=True;
Pantalla16.Visible:=False;

end;

procedure TPantalla16.Button3Click(Sender: TObject);
begin

Application.Terminate;

end;



END.
```

```
unit Unit17;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, StdCtrls, ExtCtrls, TeeProcs, TeEngine, Chart, DbChart,
  TeeFunci, Series;

type
  TPantalla17 = class(TForm)
    Label1: TLabel;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    GraficaGlobal: TChart;
    Series1: TPieSeries;
    GraficaMedia: TChart;
    Series2: TLineSeries;
    Series3: TBarSeries;
    ResultadoAuditoría: TChart;
    BarSeries1: TBarSeries;
    TeeFunction1: TAverageTeeFunction;
    LineSeries1: TPointSeries;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Pantalla17: TPantalla17;

implementation

{$R *.dfm}

USES Unit2, Unit4, Unit6, Unit7, Unit9, Unit10, Unit11, Unit13, Unit14,
  Unit15, Unit16;


procedure TPantalla17.Button1Click(Sender: TObject);
begin

Pantalla15.Visible:=True;
Pantalla17.Visible:=False;

end;

procedure TPantalla17.Button2Click(Sender: TObject);
begin
```

```
Pantalla16.Visible:=True;
Pantalla17.Visible:=False;

end;

procedure TPantalla17.Button3Click(Sender: TObject);
begin

Application.Terminate;

end;

procedure TPantalla17.FormShow(Sender: TObject);

 CONST MaxBloques= 5;
 VAR
       MediaBloqueIII: Double;
       MediaBloqueIV: Double;
begin
   GraficaGlobal.Series[0].Add(Pantalla2.Evaluate, 'Bloque I');
   GraficaGlobal.Series[0].Add(Pantalla4.Evaluate, 'Bloque II');

GraficaGlobal.Series[0].Add((Pantalla6.Evaluate+Pantalla7.Evaluate)/2,
'Bloque III');
   GraficaGlobal.Series[0].Add((Pantalla9.Evaluate + Pantalla10.Evaluate
+ Pantalla11.Evaluate)/2, 'Bloque IV');
   GraficaGlobal.Series[0].Add(Pantalla13.Evaluate, 'Bloque V');

   GraficaMedia.Series[0].Add(Pantalla2.Evaluate, 'Bloque I');
   GraficaMedia.Series[0].Add(Pantalla4.Evaluate, 'Bloque II');
   GraficaMedia.Series[0].Add((Pantalla6.Evaluate+Pantalla7.Evaluate)/2,
'Bloque III');
   GraficaMedia.Series[0].Add((Pantalla9.Evaluate + Pantalla10.Evaluate
+ Pantalla11.Evaluate)/2, 'Bloque IV');
   GraficaMedia.Series[0].Add(Pantalla13.Evaluate, 'Bloque V');

   GraficaMedia.Series[1].Add(Pantalla2.Media, 'Bloque I');
   GraficaMedia.Series[1].Add(Pantalla4.Media, 'Bloque II');
   GraficaMedia.Series[1].Add(Pantalla7.Media, 'Bloque III');
   GraficaMedia.Series[1].Add(Pantalla11.Media, 'Bloque IV');
   GraficaMedia.Series[1].Add(Pantalla13.Media, 'Bloque V');
   // ------------------------------

   MediaBloqueIII:=(Pantalla6.Evaluate+Pantalla7.Evaluate)/2;
   MediaBloqueIV:=(Pantalla9.Evaluate + Pantalla10.Evaluate +
Pantalla11.Evaluate)/2;

   ResultadoAuditoría.Series[0].Add((Pantalla2.Evaluate +
Pantalla4.Evaluate + MediaBloqueIII + MediaBloqueIV +
Pantalla13.Evaluate)/MaxBloques, 'Resultado Global');
   //ResultadoAuditoría.Series[0].Add((Pantalla2.Evaluate+10 +
Pantalla4.Evaluate +3+ MediaBloqueIII + MediaBloqueIV +
Pantalla13.Evaluate)/MaxBloques, ' Resultado Global');
```

```
   ResultadoAuditoría.Series[1].Add((Pantalla2.Media + Pantalla4.Media +
Pantalla7.Media + Pantalla11.Media + Pantalla13.Media)/MaxBloques,
'Aprobado');
   end;


end.
```

```
unit Unit18;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, Mask, StdCtrls;

type
  TPantalla18 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Label5: TLabel;
    Label6: TLabel;
    Label7: TLabel;
    Label8: TLabel;
    Label9: TLabel;
    Label10: TLabel;
    Label11: TLabel;
    Label12: TLabel;
    Label13: TLabel;
    Label14: TLabel;
    Label15: TLabel;
    Label16: TLabel;
    Label17: TLabel;
    Label18: TLabel;
    Label19: TLabel;
    Label20: TLabel;
    Label21: TLabel;
    Label22: TLabel;
    Button1: TButton;
    ComboBox1: TComboBox;
    ComboBox2: TComboBox;
    ComboBox3: TComboBox;
    ComboBox4: TComboBox;
    ComboBox5: TComboBox;
    ComboBox6: TComboBox;
    ComboBox7: TComboBox;
    ComboBox8: TComboBox;
    ComboBox9: TComboBox;
    ComboBox10: TComboBox;
    ComboBox11: TComboBox;
    ComboBox12: TComboBox;
    ComboBox13: TComboBox;
    ComboBox14: TComboBox;
    ComboBox15: TComboBox;
    ComboBox16: TComboBox;
    ComboBox17: TComboBox;
    ComboBox18: TComboBox;
    ComboBox19: TComboBox;
    ComboBox20: TComboBox;
    ComboBox21: TComboBox;
    ComboBox22: TComboBox;
```

```
    procedure Button1Click(Sender: TObject);
  private
    { Private declarations }
  public

      FUNCTION PesoPregunta (NumPre: Integer): INTEGER;
    { Public declarations }
  end;

var
  Pantalla18: TPantalla18;

implementation

USES
Unit1;

{$R *.dfm}

procedure TPantalla18.Button1Click(Sender: TObject);
VAR
   Valor, Codigo: Integer;
   Ok: Boolean;
begin

   OK:= True;

   Val (ComboBox1.Text, Valor, Codigo);
   IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN
      BEGIN
         Application.MessageBox('Error en el peso de la pregunta 1',
'Error', mb_OK);
         Ok:= False;
      END
   ELSE
       BEGIN
          Val (ComboBox2.Text, Valor, Codigo);
              IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN
                  BEGIN
                      Application.MessageBox('Error en el peso de la
pregunta 2', 'Error', mb_OK);
                      Ok:= False;
                  END
              ELSE
                  BEGIN
                      Val (ComboBox3.Text, Valor, Codigo);
                      IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN
                          BEGIN
                            Application.MessageBox('Error en el peso de
la pregunta 3', 'Error', mb_OK);
                            Ok:= False;
                          END
                      ELSE
                          BEGIN
                            Val (ComboBox4.Text, Valor, Codigo);
```

```
                              IF (Codigo <> 0) OR (NOT (Valor IN [0..9]))
THEN
                                   BEGIN
                                    Application.MessageBox('Error en el
peso de la pregunta 4', 'Error', mb_OK);
                                    Ok:= False;
                             END
                      ELSE
                             BEGIN
                                 Val (ComboBox5.Text, Valor, Codigo);
                                 IF (Codigo <> 0) OR (NOT (Valor IN
[0..9])) THEN
                                    BEGIN
                                    Application.MessageBox('Error en el
peso de la pregunta 5', 'Error', mb_OK);
                                    Ok:= False;
                                    END
                                 ELSE
                                    BEGIN
                                    Val (ComboBox6.Text, Valor, Codigo);
                                    IF (Codigo <> 0) OR (NOT (Valor IN
[0..9])) THEN
                                       BEGIN
                                       Application.MessageBox('Error en el
peso de la pregunta 6', 'Error', mb_OK);
                                       Ok:= False;
                                       END
                                    ELSE
                                      BEGIN
                                        Val (ComboBox7.Text, Valor,
Codigo);
                                        IF (Codigo <> 0) OR (NOT (Valor IN
[0..9])) THEN
                                          BEGIN
                                          Application.MessageBox('Error en
el peso de la pregunta 7', 'Error', mb_OK);
                                          Ok:= False;
                                          END
                                        ELSE
                                          BEGIN
                                            Val (ComboBox8.Text, Valor,
Codigo);
                                            IF (Codigo <> 0) OR (NOT
(Valor IN [0..9])) THEN
                                            BEGIN
                                              Application.MessageBox('Error
en el peso de la pregunta 8', 'Error', mb_OK);
                                              Ok:= False;
                                            END
                                              ELSE
                                                BEGIN
                                                  Val (ComboBox9.Text,
Valor, Codigo);
                                                   IF (Codigo <> 0) OR (NOT
(Valor IN [0..9])) THEN
                                                    BEGIN
```

```
Application.MessageBox('Error en el peso de la pregunta 9', 'Error',
mb_OK);
                                                  Ok:= False;
                                                END
                                               ELSE
                                                BEGIN
                                                  Val (ComboBox10.Text,
Valor, Codigo);
                                                  IF (Codigo <> 0) OR
(NOT (Valor IN [0..9])) THEN
                                                    BEGIN

Application.MessageBox('Error en el peso de la pregunta 10', 'Error',
mb_OK);
                                                      Ok:= False;
                                                   END
                                                  ELSE
                                                   BEGIN
                                                      Val
(ComboBox11.Text, Valor, Codigo);
                                                      IF (Codigo <> 0)
OR (NOT (Valor IN [0..9])) THEN
                                                       BEGIN

Application.MessageBox('Error en el peso de la pregunta 11', 'Error',
mb_OK);
                                                         Ok:= False;
                                                      END
                                                     ELSE
                                                       BEGIN
                                                        Val
(ComboBox12.Text, Valor, Codigo);
                                                        IF (Codigo <>
0) OR (NOT (Valor IN [0..9])) THEN
                                                          BEGIN

Application.MessageBox('Error en el peso de la pregunta 12', 'Error',
mb_OK);
                                                             Ok:= False;
                                                          END
                                                        ELSE
                                                           BEGIN
                                                              Val
(ComboBox13.Text, Valor, Codigo);
                                                              IF
(Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN
                                                                BEGIN

Application.MessageBox('Error en el peso de la pregunta 13', 'Error',
mb_OK);
                                                                   Ok:=
False;
                                                                END
                                                              ELSE
                                                               BEGIN
```

```
                                                                    Val
(ComboBox14.Text, Valor, Codigo);
                                                                    IF
(Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 14', 'Error',
mb_OK);

Ok:= False;

END
                                                                    ELSE

BEGIN

Val (ComboBox15.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 15', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox16.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 16', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox17.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN
```

```
Application.MessageBox('Error en el peso de la pregunta 17', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox18.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 18', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox19.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 19', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox20.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 20', 'Error',
mb_OK);

Ok:= False;
```

```
END

ELSE

BEGIN

Val (ComboBox21.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 21', 'Error',
mb_OK);

Ok:= False;

END

ELSE

BEGIN

Val (ComboBox22.Text, Valor, Codigo);

IF (Codigo <> 0) OR (NOT (Valor IN [0..9])) THEN

BEGIN

Application.MessageBox('Error en el peso de la pregunta 22', 'Error',
mb_OK);

Ok:= False;

END

END;

END;

END;

END;

END;

END;

END;

END;

END;

END;

END;
```

```
                                                        END;
                                                    END;
                                               END;
                                          END;
                                     END;
                               END;
                         END;
                     END;
               END;
         END;

  IF Ok THEN
      BEGIN
         Pantalla1.Visible:=True;
          Pantalla18.Visible:=False;
      END;
end;

FUNCTION TPantalla18.PesoPregunta (NumPre: Integer): INTEGER;
//Necesario que pasen el numpregunta para saber el peso

VAR PesoPre, Code: Integer;

begin

PesoPre:=0;
    IF NumPre IN [1..22] THEN
      BEGIN
        CASE NumPre OF
        1: Val (ComboBox1.Text, PesoPre, Code);    //Code hay que
ponerlo, -1 si está mal
        2: Val (ComboBox2.Text, PesoPre, Code);
        3: Val (ComboBox3.Text, PesoPre, Code);
        4: Val (ComboBox4.Text, PesoPre, Code);
        5: Val (ComboBox5.Text, PesoPre, Code);
        6: Val (ComboBox6.Text, PesoPre, Code);
        7: Val (ComboBox7.Text, PesoPre, Code);
        8: Val (ComboBox8.Text, PesoPre, Code);
        9: Val (ComboBox9.Text, PesoPre, Code);
        10: Val (ComboBox10.Text, PesoPre, Code);
        11: Val (ComboBox11.Text, PesoPre, Code);
        12: Val (ComboBox12.Text, PesoPre, Code);
        13: Val (ComboBox13.Text, PesoPre, Code);
        14: Val (ComboBox14.Text, PesoPre, Code);
        15: Val (ComboBox15.Text, PesoPre, Code);
        16: Val (ComboBox16.Text, PesoPre, Code);
        17: Val (ComboBox17.Text, PesoPre, Code);
        18: Val (ComboBox18.Text, PesoPre, Code);
        19: Val (ComboBox19.Text, PesoPre, Code);
        20: Val (ComboBox20.Text, PesoPre, Code);
        21: Val (ComboBox21.Text, PesoPre, Code);
        22: Val (ComboBox22.Text, PesoPre, Code);
        END;
END;
```

```
    PesoPregunta:=PesoPre;
end;


end.
```

```
program cuestionario;

uses
  Forms,
  Unit1 in 'Unit1.pas' {Pantalla1},
  Unit2 in 'Unit2.pas' {Pantalla2},
  Unit3 in 'Unit3.pas' {Pantalla3},
  Unit4 in 'Unit4.pas' {Pantalla4},
  Unit5 in 'Unit5.pas' {Pantalla5},
  Unit6 in 'Unit6.pas' {Pantalla6},
  Unit7 in 'Unit7.pas' {pantalla7},
  Unit8 in 'Unit8.pas' {Pantalla8},
  Unit9 in 'Unit9.pas' {Pantalla9},
  Unit10 in 'Unit10.pas' {Pantalla10},
  Unit11 in 'Unit11.pas' {Pantalla11},
  Unit12 in 'Unit12.pas' {Pantalla12},
  Unit13 in 'Unit13.pas' {Pantalla13},
  Unit14 in 'Unit14.pas' {Pantalla14},
  Unit15 in 'Unit15.pas' {Pantalla15},
  Unit16 in 'Unit16.pas' {Pantalla16},
  Unit17 in 'Unit17.pas' {Pantalla17},
  Unit18 in 'Unit18.pas' {Pantalla18},
  Unit19 in 'Unit19.pas' {Pantalla19};

{$R *.res}

begin
  Application.Initialize;
  Application.Title := 'CUESTIONARIO ISO/IEC 27002:2005 SEGURIDAD EN
REDES';
  Application.CreateForm(TPantalla19, Pantalla19);
  Application.CreateForm(TPantalla1, Pantalla1);
  Application.CreateForm(TPantalla2, Pantalla2);
  Application.CreateForm(TPantalla3, Pantalla3);
  Application.CreateForm(TPantalla4, Pantalla4);
  Application.CreateForm(TPantalla5, Pantalla5);
  Application.CreateForm(TPantalla6, Pantalla6);
  Application.CreateForm(Tpantalla7, pantalla7);
  Application.CreateForm(TPantalla8, Pantalla8);
  Application.CreateForm(TPantalla9, Pantalla9);
  Application.CreateForm(TPantalla10, Pantalla10);
  Application.CreateForm(TPantalla11, Pantalla11);
  Application.CreateForm(TPantalla12, Pantalla12);
  Application.CreateForm(TPantalla13, Pantalla13);
  Application.CreateForm(TPantalla14, Pantalla14);
  Application.CreateForm(TPantalla15, Pantalla15);
  Application.CreateForm(TPantalla16, Pantalla16);
  Application.CreateForm(TPantalla17, Pantalla17);
  Application.CreateForm(TPantalla18, Pantalla18);

  Application.Run;
end.
```

PRESUPUESTO

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Ángeles Tapiador Sanz

2.- Departamento: Informática

3.- Descripción del Proyecto:

- Titulo: **Control y Auditoría en Redes de Datos**
- Duración (meses): **12 meses**
- Tasa de costes Indirectos: **20%**

4.- Presupuesto total del Proyecto (valores en Euros):

Euros 30000

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a título informativo)	Categoría	Dedicación (hombres mes) a)	Coste hombre mes	Coste (Euro)	Firma de conformidad
		Auditor	5	1.600,00	8.000,00	
		Ingeniero Senior	1	1.450,00	1.450,00	
		Ingeniero	1	1.300,00	1.300,00	
		Hombres mes 7		**Total**	10.750,00	

[a)] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d)]
Portátil HP probook 6550	850,00	100	12	60	170,00
					0,00
					0,00
					0,00
					0,00
					0,00
				Total	170,00

[d)] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} \text{xCxD}$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado

B = periodo de depreciación (60 meses)

C = coste del equipo (sin IVA)

D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
Consultora X	S	12.000,00
	Total	12.000,00

OTROS COSTES DIRECTOS DEL PROYECTO[e)]

Descripción	Empresa	Costes imputable
	Total	0,00

[e)] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	10.750
Amortización	170
Subcontratación de tareas	12.000
Costes de funcionamiento	0
Costes Indirectos	4.584
Total	27.504

En las hojas Excel anteriores basadas en la plantilla colgada en Internet de la UC3M se puede ver una aproximación de un presupuesto global para el proyecto consistente en elaborar un guía basada en ISO 27002, y a través de ella elaborar un cuestionario para saber si la empresa a auditar conseguirá la certificación pertinente o pasar una auditoría interna. Para ello se han contratado tres personas que son un auditor, un ingeniero superior que coordine las operaciones y otro ingeniero para programar el cuestionario, usando los meses hombre se ha calculado la estimación de gastos, amortizaciones y así se ha llegado a los resultados anteriores.

En los equipos solo se ha usado un portátil y además se ha necesitado la ayuda de una consultora 'X' para labores de entrevista a responsables de área de la empresa sobre el estado de las instalaciones en las que se tire de redes de datos.

GLOSARIO

Auditoría de la gestión: la contratación de bienes y servicios, documentación de los programas, etc.

Auditoría legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoría de la seguridad física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de ésta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

Auditoría de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.

Auditoría de las comunicaciones. Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.

Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

Codificación: *encoding*, Protocolo mediante el cual se transportan o almacenan datos en un medio.

Conmutador: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (*bridges*), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Consola: La unidad en el sistema, como una terminal o teclado, a través de la cual se establece la comunicación con la computadora.

Digitalizar: Transformar una onda analógica en una señal digital que pueda almacenar una computadora.

Dirección: Se refiere a la ubicación de datos específicos dentro de la computadora ó de una memoria.

Disipador: Aparato que ayuda a eliminar el calor generado por un cuerpo, en general el microprocesador del equipo, en ocasiones con la colaboración de un ventilador. Para ello, busca tener buena conducción del calor (suelen ser de cobre) y gran superficie.

Dúplex: Indica un canal de comunicaciones capaz de transportar señales en ambas direcciones.

ECC: *Error Correction Codes, c*ódigo de corrección de errores.

Enrutador: *router*, Hardware que dirige mensajes de una red de área local a otra

Ethernet: Un estándar para redes de ordenadores muy utilizado por su aceptable velocidad y bajo coste. Admite distintas velocidades según el tipo de hardware utilizado,

siendo las más comunes 10 Mbits/s y 100 Mbits/s (comúnmente denominadas Ethernet y Fast Ethernet respectivamente).

Fibra óptica: medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

FÍFO: *First-In, First-Out*, Primero en Entrar, Primero en Salir. Método de almacenamiento y recuperación de elementos de una lista, tabla o pila, de manera que el primer elemento almacenado es el primero en recuperarse.

FireWire: "Cable de fuego" o "IEEE 1394", un estándar para la conexión de dispositivos al ordenador, tanto interna como externamente.

Firmware: Programas contenidos en un dispositivo de memoria de sólo lectura (ROM). Mezcla de hardware y software.

FTP: *File Transfer Protocol*, Protocolo para la Transferencia de Archivos. Método de transferencia de archivos a través de Internet.

Full-Duplex: Transmisión simultánea en dos direcciones.

Half-Duplex: Transmisión en una sola dirección.

Hardware: La parte física del ordenador (placa, micro, tarjetas, monitor...).

Interfaz: *interface*, Dispositivo o protocolo de comunicaciones que permite comunicar a un dispositivo con otro

LAN: *Local Area Net*, red de área local. Una red de ordenadores de tamaño medio, dispersa por un edificio.

Man: *metropolitan area network.* Red de área metropolitana.

Medio magnético: *médium*, El recubrimiento magnético o revestimiento que cubre una cinta o disco.

Medios de película delgada: *thin-film media*, Platos de disco duro que tienen una película delgada (por lo regular tres millonésimas de pulgada) de medios magnéticos depositada sobre el sustrato de aluminio.

Microprocesador: *microprocessor*, Unidad central de proceso de estado sólido muy similar a una computadora en un chip.

Módem: *MOdulador-DEModulador*, dispositivo hardware que transforma las señales digitales del ordenador en señal telefónica analógica y viceversa.

OSI: *Interconexión de Sistemas Abiertos* (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984.

Protocolo: *protocol*, Sistema de reglas y procedimientos que rigen las comunicaciones entre dos o más dispositivos. Los protocolos varían, aunque los dispositivos.

Proxy: referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Red: Conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden intercambiar información.

Sector: *sector*, Sección de una pista definida mediante marcas y números de identificación.

Semiconductor: Sustancia, como germanio o silicio, cuya conductividad es reducida a temperaturas bajas, pero mejora al incorporar pequeñas cantidades de ciertas sustancias o por la aplicación de calor, luz o voltaje.

Servidor: computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

SSH : (**S**ecure **SH**ell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TCP: Transmission Control Protocol (*Protocolo de Control de Transmisión).*

Tiempo de acceso: *access time*, El tiempo que transcurre desde el instante en que se solicita información, hasta que se recibe la respuesta.

UPS: *Uninterruptible Power Supply*, Fuente de alimentación interrumpida. También recibe el nombre de SAI (Sistema de alimentación interrumpida).

USB: *Universal Serial Bus*, bus serie universal. Tipo de conector que puede soportar hasta 126 periféricos externos, con un ancho de banda a compartir de 1,5 MB/s, lo que lo hace especialmente indicado para ratones, impresoras, joystick o módems.

Virus: Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

WAN: *Wide Area Net*, red de área ancha. Una red de ordenadores de muy gran tamaño, dispersa por un país o incluso por todo el planeta.

CONCLUSIONES

Según he ido escribiendo cada línea de este proyecto y documentándome sobre el tema he podido darme cuenta de la importancia que tiene la seguridad de la información.
Son muchas veces pequeños detalles, pero la suma de todos ellos son esenciales para el buen funcionamiento de la empresa.

Además según he ido aprendiendo cosas con el tiempo he podido ver en mi vida profesional muchas de esas cosas que escribía puestas en práctica, en algunos casos ver como sí que se cumplían y en otros casos ver muchas de las carencias o mejoras que se podrían implementar.

Con todo ello me he dado cuenta de que todavía falta mucho por hacer, y que estos temas que son actuales ahora hay que seguir investigándolos, hacer más hincapié en las políticas y sobre todo explicar a la gente más desprovista de todo lo que hay ahí y de lo fácil que es evitar males mayores muchas veces a un solo clic de ratón.

Viendo así las posibilidades de este tema de cara al futuro está claro que hay que seguir investigando. Se podrían hacer cuestionarios mucho más exhaustivos sobre este tema de comunicaciones, de todas formas la ISO 27002 da mucho de sí y cubre muchos temas de los cuales se puede indagar mucho, los cuestionarios también pueden hacer con muchas más funcionalidad, que hagan más hincapié en los temas más flojos de las empresas.

La guía que se ha elaborado trata los temas más relacionados con las redes de datos, de cara al futuro se puede profundizar mucho más en estos temas y ampliarlos añadiendo nuevos aspectos.

Cada día se investiga también más especialmente en temas de vulnerabilidades en redes, los temas del punto doce de la ISO 27002 de criptografía es un mundo muy complejo y del que queda mucho por investigar, nuevas técnicas que se vayan adaptando a las múltiples complejidades que están creando cada día, y conseguir con ello hacer que la protección de los datos y todo tipo de información sean lo más seguras posibles.

OBJETIVOS CUMPLIDOS

Para mí el mayor objetivo que he conseguido es el haberme informado sobre el tema. Haber estudiado lo que hay que hacer y lo que de verdad se hace.

Aparte de esto está clara la satisfacción personal de haber realizado el proyecto en sí, y de sentirme un poco más realizada por así decir, conocer mejor lo que hay, y saber lo que habría que hacer.

Al igual que comentaba anteriormente también me he sentido contenta conmigo misma por el hecho de ser capaz de ver cosas que no hay en algunas empresas y que habría que hacer y de dar ideas para intentar que alguno de estos temas que he redactado se puedan poner en práctica.

También a raíz de la elaboración de este proyecto he conseguido meterme en un proyecto con mi empresa para poder certificarnos en la ISO 27001. Demostrando los conocimientos que he adquirido estos meses he conseguido hacerme un hueco laboral en este mundo de la auditoría y disfrutar así de mi trabajo de cada día. También he podido ver la relación de cada línea de este proyecto con la realidad de la empresa y tener así la sensación de que el trabajo que he hecho me ha valido para mucho y por lo tanto dar gracias por lo que he aprendido.

Es por todo ello que me siento con ganas de seguir investigando de todos estos temas de seguridad y vulnerabilidades en redes y comunicaciones y sentirme mejor cada día que tenga de mi carrera profesional recordando siempre que la suma de pocos hace un mucho.

BIBLIOGRAFÍA

- **ISO/IEC 27002:2005** Dominios, *Objetivos de Control y Controles*
- **UNE-ISO/IEC 27001** *Information technology. Security techniques. Information security management systems. Requirements. (ISO/IEC 27001:2005).*
- ***Auditoría de los sistemas de información***, *Rafael Bernal*
- *www.**isaca**.org*
- *http://iso27000.wik.is/Area_Normas/ISO%2F%2FIEC_27002*
- *www.isaca.org/Knowledge-Center/**cobit**/.../**cobiT**4.1spanish.pdf*
- *www.**itil**-officialsite.com/*
- *http://www.iso27000.es/download/ControlesISO17799-2005.pdf*
- *http://www.isaca.org/PrinterTemplate.cfm?Template=/ContentManagement/HTMLDisplay.cfm&ContentID=18782&FuseFlag=1*
- *http://virmaker-dos.narod.ru/iso/36594.pdf*
- *http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18815*
- *http://www.datalawyers.com/RD_1720_2007.pdf*
- *http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18779*
- *http://www.lancelot.pecquet.org/download/design/gov/2006-ISACA-audit_standards.pdf*
- *http://lrd.yahooapis.com/_ylc=X3oDMTVnOTBsNzFlBF9TAzIwMjMxNTI3MDIEYXBwaWQDTHJlazRUTFYzNEdRVjYwVDFRYVlHeC5xMDYuMHVja2pJb3dfYzJFV3NGejhWZzVHX2xkQjRPX1YweDZPdVNOME9zVjg2a0I2BGNsaWVudANib3NzBHNlcnZpY2UDQk9TUwRzbGsDdGl0bGUEc3JjcHZpZANnZzBMLjBnZUF1MWRFWFF2NktKTDVVelgwRG1lOGtyYVNxd0FBOG93/SIG=12g5dh3lm/**http%3A//www.isaca.org/ContentManagement/ContentDisplay.cfm%3FContentID=46288*

- *http://web.frm.utn.edu.ar/comunicaciones/redes.html*
- *http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema1/tema01.htm#2.3.3.1*
- *http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29*
- *http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm*
- *http://es.wikipedia.org/wiki/Cableado_estructurado#Est.C3.A1ndares_de_Cables_UTP.2FSTP*
- www.info-ab.uclm.es/asignaturas/42602/introauditoría.pdf
- http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=54909
- *Real Academia de la Lengua Española. Diccionario [en línea]. <www.rae.es > [Consulta: 21 de abril de 2009]*

- <u>*Definiciones:*</u>
- *<http://es.wikipedia.org/wiki/Servidor>*
- *<http://es.wikipedia.org/wiki/Proxy>*
- *<http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica>*
- *<http://es.wikipedia.org/wiki/Secure_Shell>*
- *<http://es.wikipedia.org/wiki/Transmission_Control_Protocol>*
- *<http://es.wikipedia.org/wiki/Modelo_OSI>*
- *<http://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)>*

- <u>Imágenes:</u>
- *<digitalradiotech.co.uk>*
- *<advanced.comms.agilent.com>*
- *< alegsa.com.ar>*
- *< http://trevinca.ei.uvigo.es/~mdiaz/rdo01_02/TEMA_5_archivos/image004.jpg>*
- *< http://webs.um.es/barzana/II/Ii09_images/dgwzmf82_70dwgd36f3.jpg>*

- *<http://docente.ucol.mx/al008353/public_html/imagenes/coaxial.jpg>*
- *<http://radio.grupohg.es/tienda/images/RG11.jpg>*
- *<http://www.textoscientificos.com/imagenes/redes/fibraoptica-armadura.gif>*
- *<http://informatica.temuco.udelmar.cl/~lmachuca/dokuwikilucho/_media/proyectos/taller-redes/contenidos/cable-fibra-optica.jpg>*
- *<http://grupos.emagister.com/imagen/tipos_conectores_fibra_optica/t2699860.jpg>*
- *<http://www.timbercon.com/Cables-de-Fibra-Optica/Cables-de-FibraOptica.jpg>*
- *<http://www.electronica-basica.com/images/cable-fibra-optica2.jpg>*
- *< http://esp.hyperlinesystems.com/img/sharedimg/cable/stp4-c6-patch-ind.jpg>*
- *<http://es.wikipedia.org/wiki/Archivo:Topolog%C3%Ada_de_red.png>*