UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA DE INFORMÁTICA DE GESTIÓN

CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA

Curso 2009-2010

Leganés, 23 Noviembre de 2009

Autora: Esmeralda Guindel Sánchez

Tutor: Miguel Ángel Ramos González

A mi madre, a quien este proyecto
debe mucho más de lo que parece.

ÍNDICES

ÍNDICE TEMÁTICO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE ESQUEMAS

CAPÍTULO 1: CONSIDERACIONES PREVIAS

CONSIDERACIONES PREVIAS

Cada día son más las empresas que perciben su información como el motor del negocio que es, un activo estratégico que diariamente es sometido a nuevos y más graves riesgos imposibilitando que de manera efectiva, la información aporte el valor que tiene, siendo necesario vencer la inseguridad y la desconfianza que esto genera.

Virus, hackers, averías, incendios, personal descontento, errores humanos, son miles las amenazas que tienen efectos devastadores, y que generan:

- Indisponibilidad: No poder acceder a la información cuando es vital y necesaria para la toma de decisiones, por inoperatividad de las infraestructuras tecnológicas.
- Falta de confidencialidad: Información accedida por personas no autorizadas. Robo de datos de clientes, espionaje, filtraciones, fraude.
- Pérdida de integridad: alteración de la información intencionada o por error al no existir controles.
- Falta de confianza en las transacciones electrónicas con terceros, al no existir mecanismos de autenticidad y repudio.

Afrontar estas situaciones, controlando la inseguridad de nuestros sistemas de información dentro de límites aceptables por el negocio sólo es posible mediante la integración de medidas organizativas y técnicas en el marco del desarrollo de una Cultura de la Seguridad y Calidad de la Información en la empresa.

No es posible eliminar las amenazas pero sí debemos reducir la posibilidad de que actúen y el perjuicio que pueden ocasionar: Es decir, controlar el riesgo para generar seguridad y confianza, aportando veracidad y calidad a la información que se está tratando.

En una sociedad en la que los cambios se producen de manera vertiginosa, y donde la información, la tecnología y su continua innovación son el propulsor principal de una espiral de oportunidades, nuevos riesgos amenazan permanentemente a las organizaciones: la complejidad de la tecnología, información de deficiente calidad, confidencialidad comprometida etc., cuyos efectos son cada vez más graves: pérdida de confianza y oportunidad, costes económicos...

Por ello es necesario proteger la información de las organizaciones y la confianza de sus clientes ayudando al desarrollo de una verdadera cultura de la seguridad en la empresa, desarrollar un proceso de mejora continua y maduración, a través de la evaluación, metodologías de calidad, la auditoría Informática y ayudar a las empresas en el cumplimiento de las normativas.

Actualmente todas las entidades que realizan software comienzan a prestar una gran atención en la calidad y seguridad de sus productos. Esto se debe, en parte, a que los clientes cada vez son más exigentes. Además, el no tener calidad y seguridad, implica la pérdida de clientes puesto que acudirán a aquellas empresas que les ofrezcan una calidad especificada por alguna norma y una seguridad a su producto.

La calidad pretende obtener el cumplimiento de las expectativas pactadas con el/los cliente/s siguiendo los estándares establecidos para garantizar así el éxito.

La calidad depende fundamentalmente de las expectativas de los clientes, ya que son ellos quienes finalmente perciben o evalúan la calidad. Bajo este prisma, la calidad puede ser definida como la brecha entre el desempeño real y el desempeño esperado. A menor brecha, mayor calidad.

Para lograr una buena calidad, es decir para que el desempeño del producto o

servicio sea mayor o igual que las expectativas de los clientes, la clave está en conocer y comprender cuáles son esas expectativas.

El principal impacto de una mala calidad es la pérdida de rentabilidad y competitividad. Toda empresa que logra un buen nivel de calidad logra aumentar el valor de sus productos, sus ventas y su participación de mercado. Si además logra reducir sus costos, entonces la competitividad de la empresa será aún mayor.

Los datos de alta calidad deben ser completos, consistentes, exactos y actualizados. La necesidad de este tipo de datos es cada vez mayor ya que las compañías cada vez necesitan ser más eficientes en su operativa, cumplir con las normativas vigentes y contar con capacidades de monitorización que permitan que la calidad de datos se gestione como una iniciativa global.

La calidad comienza con una decisión estratégica que sólo puede ser tomada por la alta gerencia, la cual, es la decisión de competir como una compañía de categoría mundial. La calidad se concentra en lograr un desempeño de alta calidad en cada una de las facetas de la empresa.

La Seguridad informática no comprende únicamente características técnicas, sino que tiene que incorporar al personal, tanto interno como externo, a la gestión y a la organización.

Debido a la sensación de inseguridad que planea sobre la sociedad en general, también en el campo de la informática se requiere cada vez más un aumento de los niveles de Seguridad por parte de todos.

La Auditoría de Sistemas de Información comprende la revisión y la evaluación independiente y objetiva, abarcando todo o algunas de las áreas de los sistemas de información, sus estándares y procedimientos en vigor, para determinar si el sistema salvaguarda los activos, mantiene la integridad de la información y el cumplimiento de los objetivos fijados por la organización.

Teniendo en cuenta lo mencionado anteriormente, se puede observar la importancia de la Calidad y Seguridad en los entornos informáticos.

De esta importancia surge este proyecto, cuya finalidad es profundizar en el conocimiento de la calidad y de la seguridad de la información.

Se trata de relacionar ambas características, a la luz de los principales estándares aplicables, así como la auditoría como herramienta para las revisiones.

Se busca desarrollar una cultura de calidad y seguridad en el lector.

Se tratan los conceptos de calidad, seguridad y auditoría informática. La aplicación de estándares para su puesta en marcha y se dan detalles sobre su contenido. Con todo esto se pretende dar al lector un conocimiento más amplio de aquellas normas que afectan directamente a la calidad, a la seguridad y a la auditoría informática, que le permita saber que norma aplicar.

Se profundiza en estos conceptos, aplicándolos a las empresas y a la situación actual del mercado, evaluando las tendencias de la seguridad, auditoría y calidad en un futuro. Se puede observar la importancia de estos términos.

Además se le da gran importancia a la auditoría informática relacionada con la calidad y la seguridad.

El fin último es que cada persona implicada en labores informáticas esté convencida de que un trabajo bien hecho es aquel que cumple los requisitos de calidad y de seguridad necesarios, no sólo cuando ya está finalizado, sino durante toda su ejecución.

CAPÍTULO 2: INTRODUCCIÓN

2. INTRODUCCIÓN

2.1 CONCEPTO DE CALIDAD

El término calidad es ambiguamente definido y pocas veces comprendido, esto se debe a que:

- La calidad no es una sola idea, es un concepto multidimensional;
- La dimensión de calidad incluye el interés de la entidad, el punto de vista de la entidad, y los atributos de la entidad;
- Por cada concepto existen diferentes niveles de abstracción;
- Varía para cada persona en particular.

Una definición que se podría dar de calidad sería:

Conjunto de propiedades y de características de un producto o servicio, que le confieren aptitud para satisfacer unas necesidades explícitas o implícitas.

2.1.1 Evolución Histórica

Inspección/detección de errores: hasta los años 40.

Inicialmente el trabajo era artesanal y el control existente era individual, independiente de cada tarea.

En el año 1918, Ford Motor Company, monta la Primera cadena de montaje y en 1930 Laboratorios Bel la pone en marcha.

Control (estadístico) de calidad: hasta los años 80.

El mercado es poco competitivo. Precio de venta es fijado por el fabricante en función de los costes.

La principal función es impedir que el producto defectuoso llegue al cliente. Se persigue conseguir uniformidad de servicio.

El concepto de control de calidad es igual a "problema a resolver".

Se utilizan técnicas estadísticas para controlar la calidad del departamento de producción.

Se destacan en este periodo: Japón y Calidad total (1940-70). Deming, Ishikawa, Juran, Crosby,…

Garantía de calidad: a partir de los 80.

El mercado se caracteriza por ser competitivo y de oferta. El precio de venta es fijado por el mercado. Entran en juego la planificación y medida de la calidad. Se implantan modelos de calidad que afectan a todos los departamentos.

1980. Interés por la calidad en los EEUU. TQM

1987. Premio *Malcom Baldrige Quality Award*

1987. ISO 9000. A partir de las normas británicas

1992. Premio Europeo a la calidad de la EFQM.

Gestión de calidad hoy.

Se busca un impacto estratégico y la oportunidad de ventaja competitiva.

Tienen relevancia conceptos como: Planificación, fijación de objetivos, coordinación, formación, adaptación de toda la organización.

La calidad afecta a la sociedad en general: directivos, trabajadores, clientes.

Se toma como "una filosofía, una cultura, una estrategia, un estilo de gerencia de la empresa".

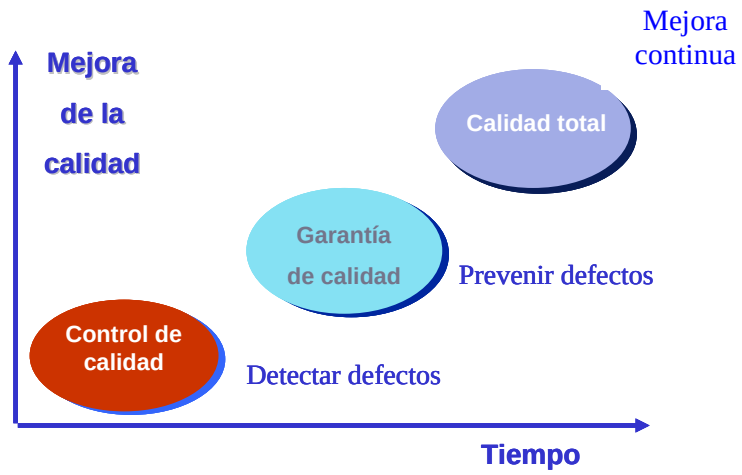


Imagen 1: Evolución Histórica

2.1.2 Algunos conceptos

Calidad: "Conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades explícitas o implícitas"

Control de calidad: "Conjunto de técnicas y actividades de carácter operativo, utilizadas para verificar los requerimientos relativos a la calidad del producto o servicio".

Garantía de calidad: "Conjunto de acciones planificadas y sistemáticas necesarias para proporcionar la confianza adecuada de que un producto o servicio satisfará los requerimientos dados sobre calidad".

Gestión de la calidad: "Aspecto de la función de gestión que determina y aplica la política de la calidad, los objetivos y las responsabilidades y que lo realiza con medios tales como la planificación de la calidad, el control de la calidad, la garantía de calidad y la mejora de la calidad".

La gestión de la calidad es responsabilidad de todos los niveles ejecutivos, pero debe estar guiada por la alta dirección.

Su realización involucra a todos los miembros de la organización.

En la gestión de la calidad, se tienen en cuenta también criterios de rentabilidad.

Sistema de gestión de la calidad: "Conjunto de la estructura de la organización, de responsabilidades, procedimientos, procesos y recursos que se establecen para llevar a término la gestión de calidad".

- Debe tener el volumen y alcance suficiente para conseguir los objetivos de calidad.
- Está fundamentalmente previsto para satisfacer las necesidades internas de la organización.).
- Para finalidades contractuales o vinculantes en la valoración de la calidad, se puede exigir que se ponga de manifiesto la realización de ciertos elementos del sistema de gestión de la calidad.

2.1.3 Calidad del Software

"*La calidad del software es el grado con el que un sistema, componente o proceso cumple los requerimientos especificados y las necesidades o expectativas del cliente o usuario*". *(*IEEE, Std. 610-1990).

"*Concordancia del software producido con los requerimientos explícitamente establecidos, con los estándares de desarrollo prefijados y con los requerimientos implícitos no establecidos formalmente, que desea el usuario*" (Pressman, 1998).

Factores que determinan la calidad del software:

Se pueden clasificar en dos grandes grupos (Pressman):

- Factores que pueden ser medidos directamente.
- Factores que sólo pueden ser medidos indirectamente.

Se centran en tres aspectos importantes de un producto software (McCall):

- Características operativas: Corrección, fiabilidad, eficiencia, seguridad (Integridad) y facilidad de uso.
- Capacidad de soportar los cambios: Facilidad de mantenimiento, flexibilidad y facilidad de prueba.
- Adaptabilidad a nuevos entornos: Portabilidad, reusabilidad e interoperabilidad.

2.2 CONCEPTO DE SEGURIDAD

2.2.1 Seguridad de la Información

La seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Los términos Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas.

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, la investigación y la situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en ordenadores y transmitida a través de las redes a otros ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o la nueva línea de productos caigan en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma. Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Integridad: Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

Disponibilidad: La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2.2.2 Seguridad Informática

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Objetivos de la seguridad informática:

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

Información: Es el objeto de mayor valor para una organización. El objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Equipos que la soportan: Software, hardware y organización.

Usuarios: Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

Análisis de riesgos

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Puesta en marcha de una política de seguridad

Generalmente se ocupa exclusivamente de asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables,

de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización (por ejemplo mediante estructura de redes en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- El usuario: causa del mayor problema ligado a la seguridad de un sistema informático.
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en el ordenador abriendo una puerta a intrusos o bien modificando los datos.
- Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso.
- Un siniestro, una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

Técnicas de aseguramiento del sistema

- Codificar la información.
- Vigilancia de red.
- Tecnologías repelentes o protectoras.

CAPÍTULO 3: CALIDAD DEL SOPORTE LÓGICO

3. CALIDAD DEL SOPORTE LÓGICO

3.1 EN LA ELECCIÓN Y APLICACIÓN DEL MÉTODO

3.1.1 Decisión

La metodología conocida como Planificar-Realizar-Comprobar-Actuar (PDCA, del inglés Plan-Do-Check-Act) se puede aplicar a todos los procesos. La metodología PDCA se puede describir del modo siguiente:

- Planificar: Establecer los objetivos y los procesos necesarios para proporcionar resultados de acuerdo con las necesidades del cliente y con las políticas de la empresa;
- Realizar: Implementar los procesos;
- Comprobar: Supervisar y evaluar los procesos y los servicios contrastándolos con las políticas, los objetivos y los requisitos e informar sobre los resultados;
- Actuar: Emprender las acciones necesarias para mejorar el rendimiento continuamente.

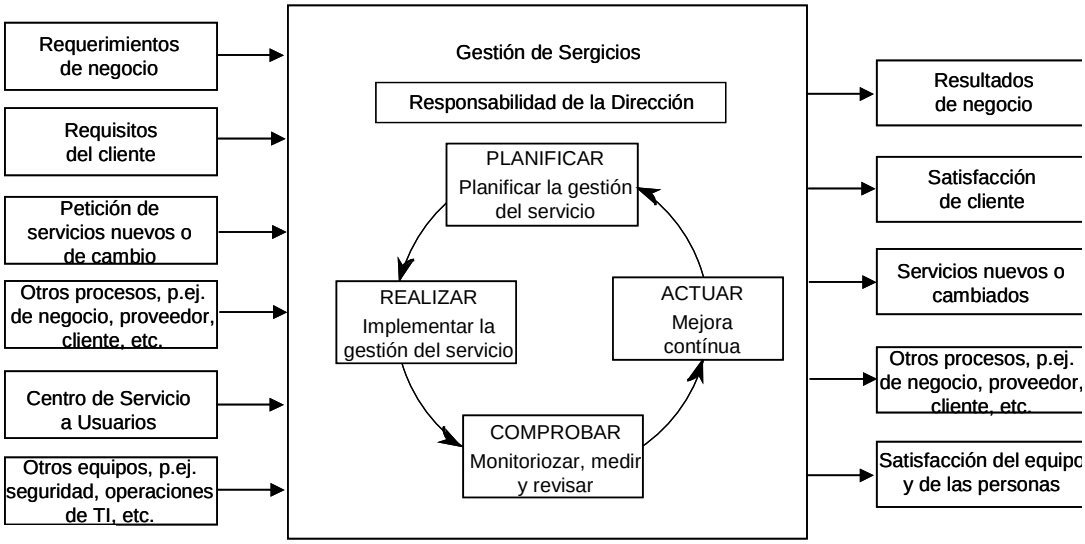


Imagen 2: Método Planificar-Realizar-Comprobar-Actuar para los procesos de gestión del servicio

3.1.2 Implantación del método

Planificación de la gestión de servicios (Planificar)

Objetivo: Planificar la implementación y la prestación de la gestión de servicios.

El alcance se debe definir como parte del plan de gestión de servicios. Por ejemplo, puede definirse según:

- la organización;
- la ubicación;
- el servicio

La gestión de servicios se debe planificar. Como mínimo, las planificaciones deberán definir lo siguiente:

- el alcance de la gestión de servicios en la organización;
- los objetivos y los requisitos que debe cumplir la gestión de servicios;
- los procesos que se deben ejecutar;
- la infraestructura de funciones y responsabilidades de gestión, incluido el propietario del proceso y la gestión de proveedores externos;
- las interfaces entre los procesos de gestión de servicios y el modo en que se deben coordinar las actividades;
- el enfoque que se debe realizar para la identificación, la evaluación y la gestión de problemas y riesgos para la consecución de los objetivos definidos;
- el enfoque para el intercambio de información con proyectos que estén creando o modificando servicios;
- los recursos, las instalaciones y el presupuesto necesario para alcanzar los objetivos definidos;
- las herramientas adecuadas para dar soporte a los procesos; y
- cómo se gestionará, auditará y mejorará la calidad del servicio.

Deberá haber una dirección de gestión clara y responsabilidades documentadas para revisar, autorizar, comunicar, implementar y mantener los planes.

Cualquier plan específico de un proceso que se elabore deberá ser compatible con este plan de gestión de servicios.

Un plan de gestión de servicios debe incluir:

- la implementación de la gestión de servicios (o de parte de la gestión de servicios);
- la facilitación de procesos de gestión de servicios;
- los cambios de los procesos de gestión de servicios;
- las mejoras de los procesos de gestión de servicios;
- los nuevos servicios (hasta el punto que afectan a los procesos incluidos en el alcance acordado de la gestión de servicios).

Implementación de la gestión de servicios y la prestación de los servicios (Realizar)

Objetivo: Implementar los objetivos y el plan de gestión de servicios.

La organización deberá implementar el plan de gestión de servicios para gestionar y prestar los servicios, incluyendo:

- la asignación de fondos y presupuestos;
- la asignación de funciones y responsabilidades;

- la documentación y el mantenimiento de políticas, planes, procedimientos y definiciones para cada proceso o conjunto de procesos;
- la identificación y la gestión de riesgos para el servicio;
- la gestión de equipos; por ejemplo, la contratación y el desarrollo del personal adecuado y la gestión de la continuidad del personal;
- la gestión de las instalaciones y el presupuesto;
- la gestión de los equipos, incluidos el servicio de atención al cliente y el de operaciones;
- un informe del progreso en comparación con los planes; y
- la coordinación de los procesos de gestión de servicios.

Supervisión, evaluación y revisión (Comprobar)

Objetivo: Supervisar, evaluar y verificar que los objetivos y el plan de gestión de servicios se cumplan.

La organización debe planificar e implementar la supervisión, la evaluación y el análisis del servicio, los procesos de gestión de servicios y los sistemas asociados. Los resultados del análisis deben proporcionar información para el programa de mejora del servicio. Entre los elementos que se deben supervisar, evaluar y analizar están los siguientes:

- los logros respecto a los objetivos de servicio definidos;
- la satisfacción del cliente;
- la utilización de recursos;
- tendencias;
- las no conformidades de mayor consideración;
- los resultados del análisis deberían de proveer entradas a un plan para la mejora del servicio.

La organización deberá aplicar métodos adecuados para la supervisión y, cuando sea necesario, la evaluación de los procesos de gestión de servicios. Estos métodos deberán demostrar la capacidad de los procesos para alcanzar los resultados planificados.

El equipo directivo deberá realizar revisiones a intervalos planificados para determinar si los requisitos de gestión de servicios:

- cumplen el plan de gestión de servicios y los requisitos de esta norma;
- se implementan y se mantienen eficazmente.

Se deberá planificar un programa de auditoría, teniendo en cuenta el estado y la importancia de los procesos y las áreas que se deben auditar así como los resultados de anteriores auditorías. Se deberán definir los criterios, el alcance, la frecuencia y los métodos de la auditoría. La selección de los auditores y la realización de las auditorías deberán garantizar la objetividad y la imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

El objetivo de las revisiones, evaluaciones y auditorías de la gestión de servicios se deberá registrar junto con las conclusiones de dichas auditorías y revisiones y las acciones correctivas que se hayan identificado.

Cualquier cuestión significativa referente a la no conformidad o a otro problema se deberá comunicar a las partes relevantes.

Mejora continua (Actuar)

Objetivo: Mejorar la eficacia y la eficiencia de la prestación y la gestión de servicios.

Política

Deberá haber una política publicada sobre la mejora del servicio. Cualquier falta de conformidad con la norma o con los planes de gestión de servicios se deberá remediar. Las funciones y las responsabilidades para las actividades de mejora del servicio se deberán definir claramente.

Gestión de las mejoras

Todas las mejoras del servicio propuestas se deberán evaluar, registrar, priorizar y autorizar. Se deberá utilizar un plan de mejora del servicio para controlar la actividad.

La organización deberá disponer de un proceso para identificar, evaluar y gestionar las actividades de mejora e informar de dichas actividades continuamente. Deberá incluir:

- las mejoras de un proceso individual que el propietario del proceso pueda implementar con los recursos de personal habituales (por ejemplo, la realización de acciones correctivas y preventivas); y
- las mejoras en toda la organización o en más de un proceso.

Actividades

La organización deberá realizar actividades para:

- recopilar y analizar datos para realizar evaluaciones de base y evaluaciones comparativas de la capacidad de la organización para gestionar y llevar a cabo la gestión de servicios;
- identificar, planificar e implementar mejoras;
- consultar a todas las partes implicadas;
- establecer objetivos para las mejoras de la calidad, los costes y la utilización de los recursos;
- considerar las aportaciones relevantes referentes a mejoras que se realicen desde todos los procesos de gestión de servicios;
- evaluar, informar de y comunicar las mejoras de servicio;
- revisar las políticas, los planes y los procedimientos de gestión de servicios siempre que sea necesario; y
- garantizar que todas las acciones aprobadas se lleven a cabo y que alcancen los objetivos deseados.

Las mejoras del servicio de más importancia se deberán gestionar como un proyecto o como varios proyectos.

3.2 RESPECTO A LA EMPRESA

3.2.1 La organización interna

El personal que realiza el trabajo en el ámbito de la gestión del servicio debería ser competente gracias a la educación recibida, a la formación, a las habilidades y a la experiencia adecuada.

El proveedor del servicio debería:

- determinar las aptitudes necesarias para cada rol en la gestión del servicio;
- asegurar que el personal es consciente de la relevancia e importancia de sus actividades dentro del más amplio contexto de negocio y de cómo contribuyen a la consecución de objetivos de calidad;
- mantener registros apropiados de la educación, la formación, las habilidades y la experiencia;
- proveer formación o llevar a cabo otras acciones que satisfagan estas necesidades;
- evaluar la efectividad en las actuaciones realizadas.

El proveedor del servicio debería abordar lo siguiente:

- **contratación**: con el objetivo de controlar la validez de los detalles de los candidatos al puesto de trabajo y de identificar la fortalezas, debilidades y habilidades potenciales de los candidatos frente a una descripción/perfil de trabajo, frente a los objetivos de la gestión del servicio y frente al conjunto de objetivos de la calidad del servicio;
- **planificación**: con el objetivo de dotar de personal a los servicios nuevos o a aquellos que se hayan ampliado, dotar de nueva tecnología, asignar personal de gestión del servicio a los equipos de desarrollo de proyecto, planificar la sucesión y rellenar los vacíos que se generen debido a rotación anticipada del personal;
- **formación y desarrollo**: con el objetivo de identificar los requisitos de formación y desarrollo dentro de un plan de formación y desarrollo y proveer su impartición en el momento oportuno y de forma efectiva.

Se deberá formar al personal en los aspectos relevantes de la gestión del servicio y se debería desarrollar el trabajo en equipo y las habilidades de liderazgo. Se debería mantener un registro de formación cronológica para cada persona, junto con descripciones de la formación proporcionada.

Los factores que se deberían considerar para establecer la combinación más adecuada:

- carácter de las competencias nuevas o modificadas: si son de corto o de medio plazo;
- tasa de cambio en las habilidades y competencias;
- picos y descensos esperados en la carga de trabajo y combinación de habilidades requeridas, datos que se deben basar en la gestión del servicio y en la planificación de mejora del servicio;
- disponibilidad de personal competente;
- tasas de rotación de personal;
- planes de formación.

3.2.2 Las personas

Jefe o director de proyecto: Es el responsable final del proyecto que está realizando. Es el enlace o interlocutor entre el cliente y la propia empresa que desarrolla la aplicación. Se encarga de la planificación de costes y plazos fijados ante el cliente, de la ejecución y control del mismo.

Jefe de equipo: Es el responsable del desarrollo de las tareas asignadas a su equipo, dirige a los trabajadores y les indica la organización, asigna nuevas tareas, suprime otras…

Analistas: Son las personas encargadas del análisis de todos los requisitos que los clientes han pedido para desarrollar la aplicación, así como intentar minimizar la dificultad que ello conlleva, resultando de su análisis una idea lo más concisa y clara posible sobre el software que se va a tener que desarrollar a continuación.

Diseñadores: Son los encargados de realizar el diseño y la estructura del proyecto que se va a tener que realizar. Éstos tendrán como base los análisis realizados por los analistas e intentarán ajustarse lo máximo posible a las funcionalidades y requerimientos que se nos ha exigido.

Programadores: Son los encargados de implementar el código fuente y objeto a partir del análisis y diseño que se ha realizado con anterioridad, así como de recopilar toda aquella documentación útil, sencilla y manejable de todo lo que se haya implementado.

Probadores software: Serán los encargados de realizar la batería de pruebas sobre la aplicación una vez finalizada la programación de la misma, para encontrar e informar sobre los fallos posibles que no se hayan solventado y futuras incidencias que se podrían producir en la utilización de la misma, así como verificar que todas las funcionalidades que han sido requeridas se hayan implementado. Dichos probadores, forman un grupo independiente al resto del equipo, para evitar que se influya negativamente (o positivamente) en el informe que se tendrá que desarrollar, y por tanto, sea lo más imparcial posible.

Instaladores: Son los encargados de instalar el software de la aplicación en cada puesto de trabajo que se necesite para el cliente. Se trasladarán para ello, hacia los lugares en los que se necesite su presencia para desarrollar esta función.

Auditor interno: Será el encargado de realizar una auditoría al final del proyecto, para comprobar si se ha realizado correctamente todas las etapas. Emitirá un informe que aportará fiabilidad y seguridad al cliente, se entregará un producto con la calidad exigida. Al igual que los probadores de software será independiente del resto del equipo por la misma razón.

3.2.3 Propuestas de estructura

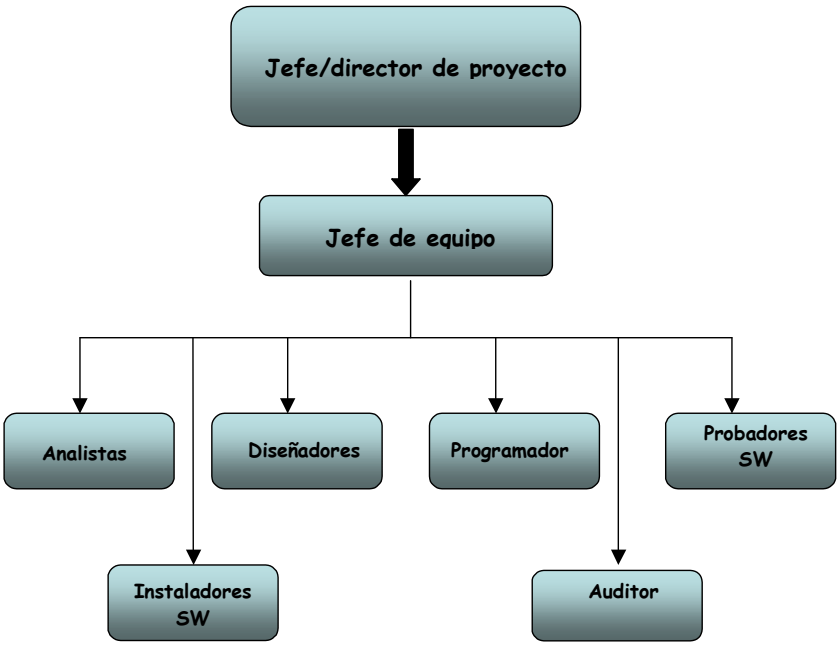


Imagen 3: Ejemplo de estructura de una empresa

El jefe de proyecto será la persona encargada de la planificación, ejecución y control del proyecto. Será el supervisor, y en encargado de impulsar que avance el proyecto.

En este gráfico se puede ver la organización de la empresa:

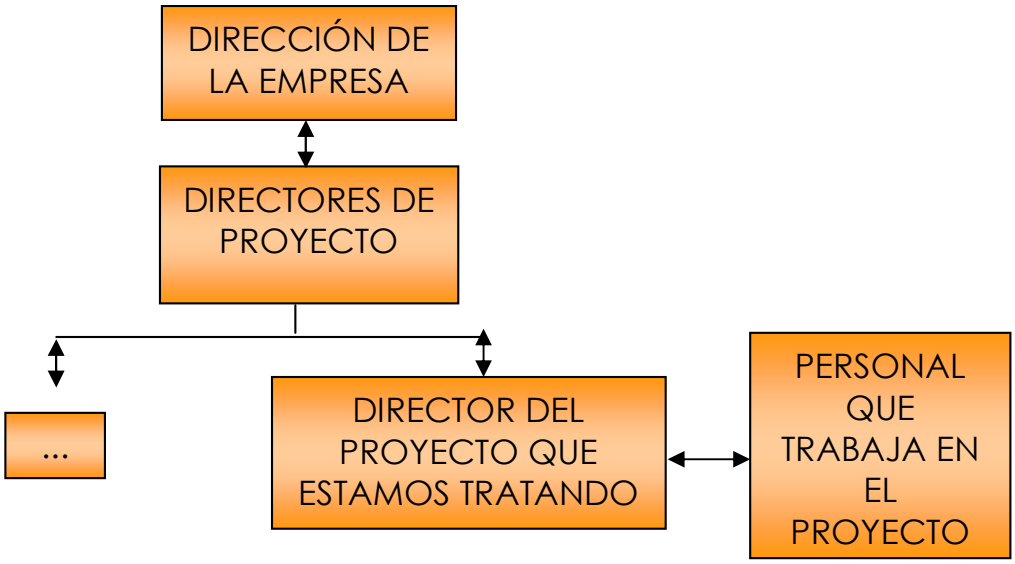


Imagen 4: Ejemplo de organización de una empresa

Como se puede observar en la imagen, la dirección de la empresa tendrá el control de los diferentes proyectos. A cargo de cada proyecto estará el director del proyecto, que estará relacionado con los clientes, y atenderá los requerimientos de éstos.

3.2.4 Canalización de las demandas de los usuarios

El objetivo es asegurar que la organización tiene, en todo momento, capacidad suficiente para cubrir la demanda acordada actual y futura del negocio.

Generará y mantendrá un plan de capacidad. Estará dirigida a las necesidades del negocio lo que incluye:

- Los requerimientos de capacidad y rendimiento actuales y previstos.
- La planificación temporal, los umbrales y costes identificados para las actualizaciones de servicios.
- La evaluación anticipada de los efectos sobre la capacidad de actualizaciones de servicio, peticiones de cambio, y nuevas tecnologías y técnicas.
- La previsión de impacto de cambios externos, por ejemplo, legislativos.
- Los datos y procesos para poder realizar análisis predictivos.

Se deben identificar métodos, procedimientos y técnicas para la monitorización de la capacidad de los servicios, el ajuste del rendimiento de los servicios y la provisión de la capacidad adecuada.

3.2.5 Resolución de conflictos

Los objetivos para la resolución deben basarse en la prioridad. La prioridad se debe basar en la repercusión y la urgencia. La repercusión se debe basar en el nivel de daño real o potencial al negocio del cliente. La urgencia se debe basar en el tiempo entre la detección del problema o la incidencia y el momento en que se produzca la repercusión sobre el negocio del cliente.

La planificación de la resolución de incidencias o problemas debe tener en cuenta, como mínimo, lo siguiente:

- la prioridad;
- las aptitudes disponibles;
- los requisitos de recursos que entren en conflicto;
- el esfuerzo/coste necesario para proporcionar el método de resolución;
- el tiempo transcurrido para proporcionar un método de resolución.

Siempre que sea necesario, la gestión de problemas deberá desarrollar y mantener soluciones provisionales para permitir a la gestión de incidencias ayudar a los usuarios o al personal a restaurar el servicio.

Un error conocido sólo se deberá cerrar cuando se haya aplicado satisfactoriamente un cambio correctivo o el error deje de existir (por ejemplo, porque el servicio ya no se utilice).

La gestión de problemas deberá tener acceso a la información sobre las áreas de negocio afectadas por problemas.

Se deberá almacenar y mantener información sobre soluciones provisionales, su aplicabilidad y su eficacia en la base de conocimientos.

3.2.5.1 Plan de contingencia

Un plan de contingencia es una "presentación para tomar acciones específicas cuando surja un evento o condición que no esté considerado en el proceso de planeación formal". Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre; es un plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia.

Consiste en un amplio estado de acciones consistentes para ser tomadas:

- **antes**, como un plan de respaldo
- **durante**, como un plan de emergencia y
- **después**, como un plan de recuperación tras un desastre.

Un adecuado plan de contingencia ayuda a la instalación de cómputo y a la organización en general a minimizar sus pérdidas en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

"El término desastre en este contexto significa la interrupción en la capacidad de acceso a la información y el procesamiento de la misma a través de los ordenadores, necesarias para la operación normal del negocio".

El plan de contingencia constituye en cierta forma un control netamente preventivo, ya que se configura como un instrumento que permite prevenir la eventualidad de un desastre, así como mantener el nivel de operación del ambiente informático; esto forma un control correctivo en la cual se materializa un riesgo, ya que se pretende reducir el impacto de éste.

Se recomienda establecer un modelo a partir de aquellas organizaciones que se han preocupado por su desarrollo y crecimiento, han establecido dentro de la estructura orgánica de la empresa una función definida para la administración de riesgos y que han obteniendo estupendos resultados, como una disminución considerable del impacto físico y económico de los riesgos dentro de la misma organización.

Este tipo de plan implica invertir tiempo, dinero y esfuerzo, y su verdadero valor sólo se podrá medir en el caso en que se presente alguna contingencia.

3.2.5.1.1 Objetivo

El propósito principal de un plan de contingencia es "mantener a la compañía y sus actividades operando aún en una situación de desastre", es decir, habilitar a la organización para responder y sobrevivir a problemas críticos o catastróficos, de forma que permita una pronta recuperación de la operación normal del centro de cómputo.

Este plan dependerá de la naturaleza de la organización, ya que inevitablemente incurrirá en costos altos. Sin embargo, es importante tener en mente que su importancia no depende de la probabilidad de un desastre, sino del efecto que éste pueda tener.

Se debe considerar que la pérdida parcial o total de las facilidades del procesamiento de datos puede causar entre otras cosas:

- Pérdidas financieras directas
- Pérdidas de la producción
- Pérdidas financieras indirectas
- Pérdidas de clientes
- Costos extras para apoyo
- Costos de compensación
- Pérdidas de control
- Información errónea o incompleta
- Bases pobres para la toma de decisiones

3.2.5.1.2 Características

En una organización, el plan de contingencia ha de contemplar dos aspectos: operacional y administrativo.

En el nivel operacional, cada usuario debe saber qué hacer cuando aparezca el problema. Asimismo debe saber la respuesta a la pregunta ¿a quién hay que llamar?

Es muy importante que el plan de contingencia determine quién debe tomar las decisiones durante la recuperación del desastre y establezca la disponibilidad y entrenamiento del personal debidamente experimentado.

En el nivel administrativo, el plan contempla aspectos como:

- Definición de riesgos y porcentajes de factibilidad a que está expuesta la organización.
- Identificación de las aplicaciones críticas para la empresa.
- Procedimiento de recuperación para la reproducción de información.
- Especificación de las alternativas de respaldo.
- Localización de los medios de respaldo.
- Responsables de los medios de respaldo.
- Archivos o bases de datos prioritarios que deben ser reconstruidos primero.
- La configuración del equipo de cómputo similar y su localización (centro de cómputo alterno o espejo).
- Localización del software de reemplazo.
- Localización de otro equipo de apoyo, tal como generadores y aire acondicionado.
- La ayuda que se puede esperar del proveedor del equipo.
- La acción a ser tomada en cada daño parcial inesperado.
- Procedimiento para la imposición de controles extraordinarios durante el desastre y hasta que regresen los sistemas a la normalidad.

En este punto también debe considerarse que para el desarrollo y mantenimiento de una buena recuperación se debe tomar en cuenta:

- Respaldo de configuración del equipo de cómputo y de la programación del software.
- Documentación y almacenamiento seguro de los procedimientos de recuperación. Un aspecto importante de la documentación es el entrenamiento de los individuos que se encargan de las operaciones de recuperación.
- Respaldo y almacenamiento seguro de los programas de forma que se pueda disponer de ellos cuando se requieran.
- Respaldo y almacenamiento seguro de los archivos de datos que sean esenciales para la operación continúa de la organización.

Al identificar un plan de contingencia como un proceso dentro de la función administrativa de riesgos, es necesario hacer consciente a todo el personal de que está involucrado en el mismo; indicar que su implantación es al mismo tiempo un dispositivo de control, el cual entra en acción en el momento en que otros controles –ya sean preventivos o detectores – fallan.

De esta manera se debe enfatizar el seguimiento de los siguientes puntos clave:

- Dar a los controles detectores las bases necesarias para el entendimiento de los esfuerzos totales que se requieren para desarrollar y mantener un efectivo plan de recuperación.
- Obtener el consentimiento de los directivos apropiados para apoyar y participar en los esfuerzos.
- Definir los requerimientos de recuperación desde la perspectiva que establece la misión de la empresa.
- Converger apropiadamente en la prevención de desastres y reducción del impacto.
- Integrar el plan de contingencia dentro de los planes generales de la organización y los procesos de desarrollo de los sistemas de forma que el plan se mantenga factible todo el tiempo.

El plan de recuperación debe cumplir con las siguientes características:

- Actual
- Entendible
- Factible
- Probado
- Documentado

3.3 CALIDAD TÉCNICA

3.3.1 Elementos para la evaluación

En la década de los 80, y ante el hecho de que la Calidad se convirtiese en el aspecto más competitivo en muchos mercados, se constituye (1988) la Fundación Europea para la Gestión de la Calidad (E.F.Q.M.), con el fin de reforzar la posición de las empresas europeas en el mercado mundial impulsando en ellas

la Calidad como factor estratégico clave para lograr una ventaja competitiva global.

Siendo el reconocimiento de los logros uno de los rasgos de la política desarrollada por la E.F.Q.M., en 1992 se presenta el Premio Europeo a la Calidad para empresas europeas. Para otorgar este premio, se utilizan los criterios del Modelo de Excelencia Empresarial, o Modelo Europeo para la Gestión de la Calidad Total, divididos en dos grupos: los cinco primeros son los Criterios Agentes, que describen cómo se consiguen los resultados (debe ser probada su evidencia); los cuatro últimos son los Criterios de Resultados, que describen qué ha conseguido la organización (deben ser medibles).

Los nueve criterios son los siguientes:

- Liderazgo: Cómo se gestiona la Calidad Total para llevar a la empresa hacia la mejora continua.
- Estrategia y Planificación: Cómo se refleja la Calidad Total en la estrategia y objetivos de la compañía.
- Gestión del personal: Cómo se libera todo el potencial de los empleados en la organización.
- Recursos: Cómo se gestionan eficazmente los recursos de la compañía en apoyo de la estrategia.
- Sistema de calidad y procesos: Cómo se adecuan los procesos para garantizar la mejora permanente de la empresa.
- Satisfacción del cliente: Cómo perciben los clientes externos de la empresa sus productos y servicios.
- Satisfacción del personal: Cómo percibe el personal la organización a la que pertenece.
- Impacto de la sociedad: Cómo percibe la comunidad el papel de la organización dentro de ella.
- Resultados del negocio: Cómo la empresa alcanza los objetivos en cuanto al rendimiento económico previsto.

Una de las grandes ventajas de la definición del modelo europeo de excelencia es su utilización como referencia para una Autoevaluación, proceso en virtud del cual una empresa se compara con los criterios del modelo para establecer su situación actual y definir objetivos de mejora.

3.4 CRITERIOS PARA EVALUAR LA CALIDAD DEL SOFTWARE

Originalmente, la calidad de un programa o sistema se evaluaba de acuerdo al número de defectos por cada mil líneas de código. En 1988, un estudio realizado en los EEUU, demostró que se introducían cerca de sesenta defectos por cada mil líneas de código (60 def/KLOC), durante las etapas de análisis, desarrollo y puesta en operación. Ya en la producción, se introducen hasta 6 def/KLOC. Hoy en día, el concepto moderno de calidad en software, requiere de una congruencia total entre los requerimientos y características del producto, para lograr una plena satisfacción del usuario. Surgen ahora componentes de la calidad tales como: Confiabilidad, soporte logístico, agilidad de respuesta, flexibilidad, facilidad de adopción, integridad, consistencia, congruencia de diseño y producto, sencillez y demás. Esto es, se quiere productos portables, fáciles de mantener y/o ampliar,

sencillo de entender, de validación accesible, compatibles con otros sistemas rápidos y efectivos, más un sinfín de características.

Por otra parte, se cuenta ahora con herramientas para producir muchas más líneas de código. Si mantienen los niveles presentes de calidad, el cuello de botella se presentará en el esfuerzo de mantenimiento que, en la actualidad, requiere el apoyar una tasa de desarrollo y producción entre tres y diez veces más rápida que antes.

CAPÍTULO 4: CALIDAD EN LA EXPLOTACIÓN

4. CALIDAD EN LA EXPLOTACIÓN

4.1 NORMAS

4.1.1 Organización Internacional para la Estandarización

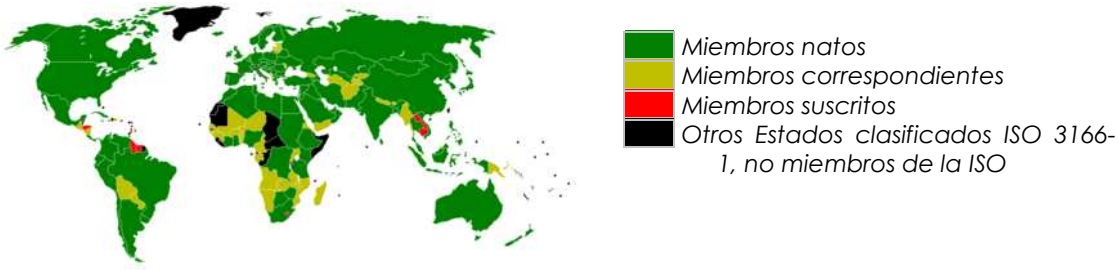


Imagen 5: Mapa mundial de Estados con comités miembros de la ISO

La Organización Internacional para la Estandarización (ISO), que nace después de la segunda guerra mundial (fue creada en 1946), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

ISO no es un acrónimo; proviene del griego ISO, que significa igual.

La ISO es una red de los institutos de normas nacionales. La Organización Internacional de Normalización (ISO), con base en Ginebra, Suiza, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental. Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país.

La Organización ISO está compuesta por tres tipos de miembros:

- Miembros natos, uno por país, recayendo el puesto, en el organismo nacional más representativo.
- Miembros correspondientes, de los organismos de países en vías de desarrollo y que todavía no poseen un comité nacional de normalización. No toman parte activa en el proceso de normalización pero están puntualmente informados acerca de los trabajos que les interesen.
- Miembros suscritos, países con reducidas economías a los que se les exige el pago de tasas menores que a los correspondientes.

4.1.2 Concepto de Normalización

La normalización es el punto de partida en la estrategia de la Calidad. Es un instrumento técnico para la implantación de un Sistema de Calidad.

Es la actividad encaminada a establecer, respecto a problemas reales o

potenciales, disposiciones destinadas a un uso común repetido, con el fin de conseguir un grado óptimo de orden. La normalización se manifiesta por la elaboración, difusión y aplicación de normas.

Una norma es el registro escrito de todos los aspectos que se han de respetar en la producción de un bien o en el suministro de un servicio.

Existen los siguientes tipos de normas: (por su ámbito de aplicación, por su contenido, por su alcance geográfico, por su contexto).

Los objetivos de la normalización de productos son los siguientes:

- Mejora de la comunicación.
- Intercambiabilidad y compatibilidad de productos.
- Reducción del surtido.
- Mejora de la seguridad, salud y bienestar.
- Protección de los intereses de los consumidores.
- Eliminación de barreras al comercio.

Entre los numerosos objetivos de la normalización de procesos (procedimientos) se citan los siguientes:

- Mejora de la comunicación interna.
- Racionaliza los procesos internos.
- Elimina una parte de los costos asociados a la mala Calidad. Al mismo tiempo reduce la variabilidad de la producción, aumentando la satisfacción del cliente.
- Como un instrumento de Gestión de la Calidad, contribuye a mejorar la productividad.
- Permite conocer el punto de partida para la mejora posterior.

4.2 NORMAS EN CALIDAD DE EXPLOTACIÓN

- ISO 9001: En esta norma se especifica:
  - Con respecto al consumidor: La alta dirección debe asegurar que se determinan las necesidades y expectativas de los clientes, que además se convierten en requerimientos y que se cumplen, con el objetivo de alcanzar la satisfacción de los clientes.
  - Administración del recurso: La entidad deberá determinar y aportar los recursos necesarios y a tiempo para implantar y mejorar los procesos del Sistema de Gestión de la Calidad y además para conseguir la satisfacción de los clientes.
  - Realización del producto: La secuencia de procesos y subprocesos requeridos para obtener el producto, y cómo se llevan a cabo.
    - *Planificación:* En la planificación se establecen los objetivos de la calidad para el producto, proyecto o contrato. Además se crea la necesidad de establecer procesos y documentación, así como recursos e instalaciones específicos para el producto.
      - Se planifica la verificación y validación, y criterios de evaluación.
      - Se realizan los registros para aportar confianza de la conformidad de los procesos, y de los productos resultantes.

- *El cliente con los procesos relacionados:* Se determinan los requerimientos de los clientes, y los no especificados pero necesarios según el uso, y requerimientos legales y regulatorios.

  Se realiza una revisión de los requerimientos (antes de la aceptación del cliente).

  Se realiza la comunicación a los clientes:

  - Información del producto.
  - Peticiones.
  - Contratos.
  - Variaciones.
  - Respuestas del cliente, inclusive quejas.

- Producción y servicio de operaciones:

  - *Operaciones de control:* La entidad deberá controlar la producción y las operaciones de servicio a través de:
    - La disponibilidad de información que especifique las características del producto.
    - Instrucciones, si es necesario.
    - El uso y mantenimiento de equipos adecuados para producción y operaciones de servicio.
    - La disponibilidad y uso de dispositivos de medida y de seguimiento.
    - La implementación de actividades de seguimiento.
    - La implementación de procesos definidos para actividades de lanzamiento, entrega y post-entrega.
  - *Preservación del producto:* la entidad preservará la conformidad del producto con los requerimientos del cliente durante el proceso interno y la entrega en destino.
  - *Validación de procesos:* la entidad validará procesos de producción y de servicio cuando las salidas resultantes no puedan verificarse por medidas o seguimientos posteriores. Estos incluye los procesos cuando las deficiencias puedan aparecer, sólo cuando el producto está ya en uso o el servicio ya se ha entregado.

- Control de dispositivos de medida y de seguimiento: la entidad deberá identificar las medidas a realizar, los dispositivos de medida y de seguimiento para asegurar la conformidad del producto con los requerimientos especificados (comprobar que realmente funciona como habíamos dicho).

- La medida y control: La entidad analizará información sobre la satisfacción o insatisfacción del cliente como una de las medidas de la utilidad del Sistema de Gestión de la Calidad puesto que la satisfacción del cliente es lo más importante ya que nos indicará si la calidad es adecuada.

  Se determinarán las metodologías para obtener y usar esta información:

  - Quejas.

- Sondeos, entrevistas, cuestionarios.
- Organizaciones de consumidores / clubes de usuarios.
- "benchmarking"

Control de la no conformidad: la entidad debe asegurarse de que se identifica el producto que no cumple los requerimientos y se controla para evitar un uso o distribución no adecuados. Dicho producto se corregirá y estará sujeto a reverificación posterior para demostrar su conformidad.

Cuando las no conformidades se detectan después de la entrega o cuando ha empezado el uso, la entidad iniciara acciones relativas a las consecuencias de la no conformidad.

Con frecuencia se requerirá que las rectificaciones se comuniquen a los clientes, usuarios finales, etc.

- *Análisis de los datos:* La entidad recogerá y analizará datos apropiados para determinar la adecuación y eficacia del Sistema de Gestión de la Calidad y para identificar mejoras. Se realizará dicho análisis para aportar información sobre:
  - Satisfacción o insatisfacción del cliente.
  - Conformidad con los requerimientos del cliente.
  - Posibles causas.
  - Características de procesos, de productos, y sus tendencias.
  - Proveedores.
- *Acción correctiva:* la entidad aplicará acciones correctivas para eliminar la causa de las no conformidades, para prevenir repeticiones. Dichas acciones serán proporcionales al impacto de los problemas encontrados.

  El procedimiento documentado definirá requerimientos para:
  - Identificar las no conformidades (incluso quejas de clientes).
  - Determinar las causas de no conformidades.
  - Evaluar la necesidad de acciones para garantizar que no se repiten las no conformidades.
  - Determinar e implementar las acciones correctivas necesarias.
  - Registrar los resultados de las acciones emprendidas.
  - Revisar las acciones correctivas realizadas.

- ISO / IEC 15504: Se especifica:
  - Procesos: los agrupa en:
    - *Procesos primarios del ciclo de vida*.

      Con categorías de procesos:
      - Cliente/Suministrador (CUS) : procesos que afectan al cliente
      - Ingeniería (ENG): procesos de especificación, implantación o mantenimiento del producto software.

- *Procesos de soporte del ciclo de vida de soporte:* con categoría:
  - Soporte (SUP): procesos utilizables por cualquiera de los otros procesos, incluso otros de soporte en diferentes puntos del ciclo de vida.
- *Procesos organizativos del ciclo de vida.* Categorías:
  - Administración (MAN): Dirección de procesos que contiene prácticas que pueden usar cualquiera que gestione cualquier tipo de proyecto o proceso dentro del ciclo de vida.
  - Organización (ORG): procesos que establecen las metas "de negocio" de la entidad, y que desarrollan procesos, productos y activos de recursos que, cuando se usan en proyectos de la entidad ayudan a la entidad a alcanzar sus metas "de negocio".
- *Aseguramiento de la calidad:* Para aportar garantía de que los productos y procesos de un proyecto cumplen con los requerimientos especificados y los planes establecidos...
- Proceso de administración de la calidad: el propósito es verificar la calidad de los productos y/o servicios del proyecto y asegurarse de que satisfacen al cliente.

4.3 CONTROLES INTERNOS

Los sistemas que se utilizan para dirigir, procesar, clasificar, la información sensible deben asegurar la responsabilidad individual, siempre que se invoque una política de seguridad obligatoria o discrecional. Además, con el fin de asegurar la responsabilidad debe existir un agente autorizado y competente, que tenga acceso y evalúe la responsabilidad de la información por medios seguros, dentro de una cantidad de tiempo razonable.

El objetivo del control de la responsabilidad se relaciona con la revisión y conduce al objetivo siguiente:

Un sistema informático confiable debe proveer al personal autorizado la capacidad de revisar cualquier acción en la que pueda potencialmente causar el acceso, generación, o efectúe el desbloqueo de la información clasificada o sensible. Los datos de la auditoría serán adquiridos selectivamente tomando en cuenta las necesidades de la revisión de una instalación y/o de una aplicación determinada. Sin embargo, debe haber suficiente seguridad en los datos de la auditoría que permitan rastrear los sucesos, los individuos específicos (o los procesos) que ha efectuado las acciones.

Un método para llevar a cabo controles, sería a través de realizar auditorías, como se explicará más adelante.

Para la planeación de la auditoría deben tenerse en cuenta varios aspectos:

- La cantidad de datos.
- La seguridad.
- El personal.
- Aspectos de seguridad en la auditoría.
- Aspectos generales de la revisión.
- El tiempo destinado a la auditoría.

Además se requiere de eficiencia debido al volumen de datos que se manejan.

La cantidad de los datos es un factor importante. Este elemento va a determinar la capacidad del sistema y la complejidad de la misma, en cuanto al volumen de datos almacenados o los elementos que intervienen.

Además de otros controles que puedan ser justificables y aconsejados en cualquier parte de la ISO/IEC 20000 (p. e.: en la continuidad del servicio), los proveedores del servicio deberían aplicar los siguientes controles como una buena práctica en gestión de la seguridad de la información:

- la alta dirección debería definir la política de seguridad de la información, comunicarla a su personal y a sus clientes y asegurarse de que se implanta eficazmente;
- los roles y las responsabilidades para la gestión de la seguridad de la información se deberían definir y asignar a un puesto de trabajo;
- un representante del equipo de dirección (el rol puede ser desempeñado por el responsable sénior) debería supervisar y mantener la eficacia de la Política de Seguridad de la Información;
- el personal que ejerza un rol significativo en seguridad debería recibir formación en seguridad de la información;
- todo el personal debe ser concienciado acerca de la política de seguridad de la información;
- debería haber apoyo de expertos en la evaluación de riesgos y en la implementación de controles;
- los cambios no deberían comprometer la operación efectiva de los controles;

Los incidentes de seguridad de la información se deberían reportar siguiendo los procedimientos de gestión del incidente y, también, se debería iniciar una respuesta a dichos incidentes.

4.4 EVALUACIÓN DE RESULTADOS

La organización debe planificar e implementar la supervisión, la evaluación y el análisis del servicio, los procesos de gestión de servicios y los sistemas asociados. Los resultados del análisis deben proporcionar información para el programa de mejora del servicio. Entre los elementos que se deben supervisar, evaluar y analizar están los siguientes:

- los logros respecto a los objetivos de servicio definidos;
- la satisfacción del cliente;
- la utilización de recursos;
- tendencias;
- las no conformidades de mayor consideración;
- los resultados del análisis deberían de proveer entradas a un plan para la mejora del servicio.

Además de las actividades de gestión de servicios sobre la evaluación y el análisis, es posible que la alta gerencia necesite recurrir a auditorías internas y otros tipos de comprobaciones. Al decidir la frecuencia de dichas auditorías internas y comprobaciones, se deberá tener cuenta, entre otros factores, el nivel de riesgo implicado en un proceso, su frecuencia de realización y su historial de problemas.

Al igual que las auditorías de certificación y recertificación externas, las auditorías y comprobaciones internas se deberán planificar, llevarse a cabo de modo competente y registrar del mismo modo que se realizaría en una auditoría externa independiente.

4.5 SEGURIDAD

Un sistema de cómputo es seguro si se puede confiar en él, si su software se comporta como se espera que lo haga, y si la información almacenada en él se mantiene inalterada y accesible durante tanto tiempo como su dueño lo desee.

Sobre este aspecto, la seguridad busca consolidar la confidencialidad, integridad, autenticidad y disponibilidad de la información. De igual forma, la seguridad informática busca mantener y conservar la operatividad de la organización y de su sistema a partir del resguardo de sus recursos.

Confidencialidad

Un sistema de cómputo no debe permitir que la información contenida en él sea accesible a nadie que no tenga la autorización adecuada.

Integridad y Autenticidad

Un sistema de cómputo no debe permitir modificaciones no autorizadas a los datos o la información contenida en él. Este punto comprende cualquier tipo de modificaciones:

- Por errores de hardware y/o software.
- Causadas por alguna persona de forma intencional.
- Causadas por alguna persona de forma accidental.

La Autenticidad se maneja en cuestión de telecomunicaciones, e implica disponer de un medio para verificar quién envía la información, así como poder comprobar que los datos no fueron modificados durante su transferencia.

Disponibilidad

La información puede estar sana y salva en el sistema, pero de poco sirve si los usuarios no tienen acceso a ella. La disponibilidad significa que los recursos del sistema, tanto de hardware como de software, se mantendrán funcionando de forma eficiente, y que los usuarios lo podrán utilizar en el momento que lo necesiten. También significa que el sistema sea capaz de recuperarse rápidamente en caso de ocurrir un problema de cualquier especie.

4.5.1 Objetivos de las medidas de seguridad

Pueden ser vistos como una serie de niveles de control: si un nivel falla, entonces otro nivel toma posesión u ocupa su lugar y continúa con la operación del sistema, de forma que el impacto global que pudiera ocasionar la falla se reduce. Estos objetivos son:

- **Disuadir.** En este nivel la meta es prevenir cualquier tipo de amenaza o desastre que pueda ocurrir.
- **Detectar.** La disuasión total generalmente no se consigue; por lo tanto, en este nivel se establecen métodos de monitoreo y vigilancia que reporten cualquier riesgo o peligro, y que permitan tomar las acciones correctivas pertinentes.
- **Minimizar el impacto de pérdida o desastre.** Si un accidente o contratiempo ocurre, deben establecerse procedimientos que ayuden

a reducir la pérdida o el daño.

- **Investigar.** Si la pérdida ocurre, puede realizarse una investigación que ayude a determinar lo que pasó. La información que derive de esta investigación puede servir para futuras planeaciones de seguridad.
- **Recuperar.** Las medidas de seguridad implican que debe de haber un plan de acción para recuperación en caso de que un accidente o desastre ocurra (sea cual fuere su causa), y hacerlo de la manera más pronta posible.

4.5.2 Consideraciones sobre Seguridad

La seguridad en cómputo de cualquier otro tipo cuesta tiempo, dinero y, sobre todo, esfuerzo. Es posible obtener en general ciertos niveles mínimos de seguridad sin hacer un gasto considerable. Pero, el logro de protección adicional requiere niveles de gastos más altos y, con frecuencia, retribuciones menores. La economía siempre resulta necesaria y es importante asegurarse de que existe una relación coste/beneficio razonable con respecto a las medidas de seguridad.

Para ello es necesario establecer prioridades. Entre estas tenemos:

¿Qué se quiere proteger?

Es muy importante determinar el valor del hardware y las tareas que realiza (qué tan importante es para la organización en que se está trabajando). Esta valoración debe hacerse de forma individual, pues lo que es valioso para algunos no lo es para otros.

¿Contra qué se quiere proteger?

Para no incurrir en gastos innecesarios, es importante determinar cuáles son los riesgos reales a los que está expuesto el equipo de cómputo.

La seguridad efectiva debe garantizar la prevención y detección de accidentes, ataques, daños por causas naturales, así como la existencia de medidas definidas para afrontar los desastres y lograr el restablecimiento de las actividades.

¿Cuánto tiempo, dinero y esfuerzo se está dispuesto a invertir?

Se refiere a la cantidad de recursos que dispone o que está dispuesta a invertir la organización, o que determinará en última instancia las medidas que se van a tomar.

Estos recursos son:

- ***Tiempo.*** Para tener un nivel de seguridad alto es necesario que alguien dedique tiempo a configurar los parámetros de seguridad del sistema, el ambiente de trabajo de los usuarios, revisar y fijar los permisos de acceso a los archivos, ejecutar programas de monitoreo de seguridad, revisar las bitácoras del sistema, etc.
- ***Esfuerzo.*** Establecer y mantener un nivel adecuado de seguridad puede significar un esfuerzo considerable por parte del encargado, sobre todo si ocurren problemas de seguridad.
- ***Dinero.*** El tener a alguien que se encargue de la seguridad en forma responsable cuesta dinero. De igual forma cuesta dinero adquirir los productos de seguridad que se vayan a utilizar, ya sean programas o equipos.

Es importante también analizar los costos que tendrían la pérdida o acceso

no autorizado a la información. Dependiendo de esto, y en el caso de que alguien tenga acceso no autorizado, el efecto puede ser pérdidas monetarias o poner en peligro la seguridad nacional, sólo como ejemplos drásticos.

Debido a lo anterior, las consideraciones que deben tomarse en cuenta al planear la seguridad son:

- Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.
- Justificación de las medidas de seguridad en cuanto al costo que representa.

Se debe tomar en cuenta que es prácticamente imposible hacer que un sistema sea totalmente seguro, debido a que no se puede prever todas las posibles amenazas aún cuando la seguridad se incremente a niveles muy altos, ya que siempre habrá una manera de obtener acceso no autorizado.

Para determinar de una forma correcta la seguridad con la que se debe contar se debe estudiar desde dos puntos de vista: el primero va a constar de los elementos administrativos que toda organización desarrolla para un buen control, y el segundo se compondrá de los elementos que integran la seguridad física.

4.5.3 Normas obligatorias

El objetivo es gestionar la seguridad de la información de manera efectiva para todas las actividades del servicio.

La seguridad de la información es el resultado de un sistema de políticas y procedimientos designados a identificar, controlar y proteger la información y cualquier equipamiento empleado junto con su almacenamiento, transmisión y procesamiento.

Nota: ISO/IEC 27002 presenta una guía sobre gestión de la seguridad de la información.

Alguien de la Dirección con la autoridad apropiada deberá aprobar una política de seguridad de la información que deberá ser comunicada a todo el personal implicado y a los clientes cuando sea adecuado.

Controles adecuados de seguridad deben funcionar para:

- Implementar los requisitos de la política de seguridad de la información.
- Gestionar los riesgos asociados al acceso al servicio o a los sistemas.

Los controles de seguridad deben estar documentados. La documentación debe describir los riesgos a los que están asociados los controles, y la manera de utilizarlos y el mantenimiento de los mismos. El impacto de los cambios sobre los controles debe ser valorado antes de que los cambios sean implementados.

Los acuerdos que impliquen el acceso de terceros a los sistemas de información y a los servicios deben basarse en un acuerdo formal que defina todos los requisitos de seguridad necesarios.

Las incidencias de seguridad deben ser comunicadas y registradas de acuerdo a los procedimientos de gestión de incidencias tan pronto como sea posible. Se deben poner en marcha procedimientos para asegurar que todas las incidencias de seguridad son investigadas, y que se toman medidas al respecto. Se deben poner en marcha mecanismos para permitir cuantificar y monitorizar los tipos, volúmenes e impacto de las incidencias y el mal funcionamiento de la seguridad, y para ofrecer entradas al plan de mejoras.

El personal del proveedor del servicio con roles de especialista en seguridad de la información debería estar familiarizado con la norma UNE-ISO/IEC 17799, Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la gestión de la seguridad de la información.

El proveedor del servicio debería:

- mantener un inventario de los activos de información (por ejemplo, ordenadores, sistemas de comunicación, documentos y otra información) que son necesarios para la prestación de los servicios;
- clasificar cada activo de acuerdo con su criticidad para el servicio y el nivel de protección que requiera, y nombrar a un propietario para ser responsable de proveer dicha protección;
- la responsabilidad para la protección de los activos debería recaer en el propietario de dichos activos, aunque estos pueden delegar las responsabilidades de la gestión diaria de la seguridad.

La evaluación de los riesgos de seguridad debería:

- ser realizada con una periodicidad acordada;
- ser registrada;
- ser mantenida durante los cambios (cambios de necesidades del negocio, de procesos o de configuraciones)
- ayudar a entender qué podría impactar uno de los servicios gestionados;
- proveer de información para las decisiones referentes a los tipos de controles a establecer.

Los riesgos para los activos de información se deberían evaluar en función de:

- su naturaleza (p. e.: funcionamiento defectuoso del software, errores de operación, fallos de comunicación);
- probabilidad;
- impacto potencial para el negocio;
- experiencias pasadas.

Al evaluar los riesgos, se debería prestar atención a los siguientes puntos:

- revelación de información sensible a partes no autorizadas;
- información inexacta, incompleta o inválida (p. e.: información fraudulenta);
- información que quede inservible para su uso (p. e.: debido a un corte de energía eléctrica);
- daño físico o destrucción de los equipos necesarios para proveer los servicios.

También se deberían tener en cuenta los objetivos de la política de seguridad de la información, las necesidades para satisfacer los requisitos específicos de los clientes respecto a la seguridad (p. e.: niveles de disponibilidad) y los requisitos legales o regulatorios que apliquen.

4.5.4 Errores más frecuentes

Uno de los errores más frecuentes, son los cambios erróneos referentes al servicio. Par evitar esto, se deben tener en cuenta lo siguientes planes:

- la contratación y formación del personal;
- la reubicación;
- la formación al usuario;
- las comunicaciones sobre los cambios;
- los cambios en la naturaleza de la tecnología a la que se da soporte;
- el cierre formal de los servicios.

Otro error común será el no asegurar que los compromisos, de continuidad y disponibilidad, acordados con los clientes puedan cumplirse bajo todas las circunstancias.

- La gestión de la disponibilidad debería:
  - supervisar y registrar la disponibilidad del servicio;
  - mantener datos históricos precisos;
  - realizar comparaciones con los requisitos definidos en los ANSs para identificar no conformidades con los objetivos de disponibilidad acordados;
  - documentar y revisar las no conformidades;
  - predecir la disponibilidad a futuro;
  - cuando sea posible, predecir los potenciales problemas y realizar acciones preventivas.

Se debería asegurar la disponibilidad de todos los componentes del servicio, registrando las acciones correctoras y llevándolas a cabo.

- El proveedor del servicio debería acordar con cada grupo de clientes y servicios:
  - los periodos máximos aceptables de pérdida continuada del servicio;
  - los periodos máximos aceptables de degradación del servicio;
  - los niveles aceptables de degradación del servicio durante un periodo de recuperación del servicio.

La estrategia de continuidad debería ser revisada con una periodicidad acordada, al menos anualmente.

Cualquier cambio a la estrategia debería ser acordado formalmente.

- El proveedor del servicio debería asegurar que:
  - los planes de continuidad tienen en cuenta las dependencias entre servicios y componentes de los sistemas;
  - se registran y mantienen los planes de continuidad del servicio y el resto de documentos requeridos para dar soporte a la continuidad del servicio;
  - la responsabilidad para activar los planes de continuidad está claramente asignada y los planes establecen claramente la

responsabilidad para la toma de las acciones necesarias frente a cada objetivo;

- las copias de seguridad de los datos, los documentos y el software y cualquier equipo y personal necesario para la restauración del servicio están disponibles de forma rápida ante un desastre o un fallo importante del servicio;
- al menos una copia de todos los documentos relativos a la continuidad del servicio debería estar almacenada y mantenida en una localización remota segura, junto al equipamiento que sea necesario para permitir su uso;
- el personal conoce y asume su rol para activar y/o ejecutar los planes y tiene acceso a la documentación relativa a la continuidad del servicio.

Los planes de continuidad del servicio y la documentación relacionada (por ejemplo los contratos) deberían estar ligados a los procesos de gestión de cambios y de gestión de los contratos.

La no existencia de una política para la gestión financiera de los servicios. La política debería definir los objetivos a ser cumplidos por la realización de los presupuestos y la contabilidad.

La política debería definir también el nivel de detalle al que se realice la realización de los presupuestos y la contabilidad, teniendo en cuenta:

- los tipos de costes a ser contabilizados;
- el reparto de los gastos generales, por ejemplo reparto en partes iguales, reparto porcentual o reparto basado en el tamaño de los elementos variables empleados;
- la granularidad del negocio del cliente, por ejemplo unidades de negocio tomadas como una sola, divididas en departamentos o según las diferentes ubicaciones;
- las reglas para manejar las variaciones frente al presupuesto, por ejemplo el nivel de variación necesario para que se escale a la alta dirección;
- los enlaces o vinculación con la gestión de nivel de servicio.

El no establecer un proceso para gestionar las implicaciones de las variaciones frente al presupuesto.

Desconocimiento en términos de lo que el negocio va a necesitar para dar servicio a sus clientes para los requisitos de servicio actuales y esperados del negocio.

El proceso debería ofrecer soporte directo al desarrollo de servicios nuevos y a la modificación de los mismos realizando dimensionamiento y modelización de servicios.

Mala gestión de la seguridad de la información de manera efectiva para todas las actividades del servicio.

- El proveedor del servicio debería:
  - mantener un inventario de los activos de información (por ejemplo, ordenadores, sistemas de comunicación, documentos y otra información) que son necesarios para la prestación de los servicios;
  - clasificar cada activo de acuerdo con su criticidad para el servicio y el nivel de protección que requiera, y nombrar a un propietario para

ser responsable de proveer dicha protección;

- la responsabilidad para la protección de los activos debería recaer en el propietario de dichos activos, aunque estos pueden delegar las responsabilidades de la gestión diaria de la seguridad.

- La evaluación de los riesgos de seguridad debería:
  - ser realizada con una periodicidad acordada;
  - ser registrada;
  - ser mantenida durante los cambios (cambios de necesidades del negocio, de procesos o de configuraciones)
  - ayudar a entender qué podría impactar uno de los servicios gestionados;
  - proveer de información para las decisiones referentes a los tipos de controles a establecer.

Malos controles en la gestión.

Se deberían aplicar los siguientes controles como una buena práctica en gestión de la seguridad de la información:

- la alta dirección debería definir la política de seguridad de la información, comunicarla a su personal y a sus clientes y asegurarse de que se implanta eficazmente;
- los roles y las responsabilidades para la gestión de la seguridad de la información se deberían definir y asignar a un puesto de trabajo;
- un representante del equipo de dirección (el rol puede ser desempeñado por el responsable sénior) debería supervisar y mantener la eficacia de la Política de Seguridad de la Información;
- el personal que ejerza un rol significativo en seguridad debería recibir formación en seguridad de la información;
- todo el personal debe ser concienciado acerca de la política de seguridad de la información;
- debería haber apoyo de expertos en la evaluación de riesgos y en la implementación de controles;
- los cambios no deberían comprometer la operación efectiva de los controles;
- los incidentes de seguridad de la información se deberían reportar siguiendo los procedimientos de gestión del incidente y, también, se debería iniciar una respuesta a dichos incidentes.

Mala revisión del servicio.

El proveedor del servicio debería planificar y registrar todas las reuniones formales, registrar los problemas tratados y realizar el seguimiento de las acciones acordadas.

4.5.5 Pasos a dar para la gestión de un problema

Se debería definir claramente qué constituye un incidente grave y quién está capacitado para llevar a cabo cambios en el funcionamiento habitual del proceso de incidentes/problemas.

Todos los incidentes graves deberían tener en todo momento un

gerente responsable claramente definido.

Minimizar las interrupciones de servicio de cara al negocio mediante la identificación proactiva y el análisis de las causas de los incidentes y la gestión de los problemas hasta su cierre.

El proceso de gestión del problema debería investigar las causas subyacentes de los incidentes.

Se deberían clasificar los incidentes para ayudar a determinar las causas de los problemas. La clasificación puede hacer referencia a problemas y cambios existentes

La información sobre soluciones provisionales, arreglos permanentes o el progreso del problema se debería comunicar a las partes afectadas o puede ser requerida para dar soporte a los servicios afectados.

Se debería realizar un seguimiento del progreso de todos los problemas.

Todos los problemas se deberían escalar a las partes apropiadas. El proceso debería cubrir:

- el registro de los cambios de las identidades de los responsables de la resolución de problemas durante el ciclo de vida de cada problema;
- la identificación de incidentes que rompan los objetivos de nivel de servicio;
- la distribución de información en cascada a clientes y colegas para que puedan emprender las acciones adecuadas para minimizar la repercusión del problema no resuelto;
- la definición de los puntos de escalado;
- el registro de los recursos empleados y de las acciones realizadas.

Además, se deberían realizar revisiones de los problemas siempre que la investigación para esclarecer problemas no resueltos, inusuales o de gran repercusión las justifique. La finalidad de estas revisiones es encontrar mejoras para el proceso y evitar la repetición de incidentes o errores.

4.6 TÉCNICAS AVANZADAS DE GESTIÓN DE LA CALIDAD

4.6.1 Benchmarking

El Benchmarking es un proceso a partir del cual se identifican las mejores prácticas en un determinado proceso o actividad, se analizan y se incorporan a la operativa interna de la empresa.

Dentro de la definición de Benchmarking como proceso clave de gestión a aplicar en la organización para mejorar su posición de liderazgo encontramos varios elementos clave:

- Competencia, que incluye un competidor interno, una organización admirada dentro del mismo sector o una organización admirada dentro de cualquier otro sector.
- Medición, tanto del funcionamiento de las propias operaciones como de la empresa Benchmark, o punto de referencia que vamos a tomar como organización que posee las mejores cualidades en un campo determinado.

- Representa mucho más que un Análisis de la Competencia, examinándose no sólo lo que se produce sino cómo se produce, o una Investigación de Mercado, estudiando no sólo la aceptación de la organización o el producto en el mercado sino las prácticas de negocio de grandes compañías que satisfacen las necesidades del cliente.
- Satisfacción de los clientes, entendiendo mejor sus necesidades al centrarnos en las mejores prácticas dentro del sector.
- Apertura a nuevas ideas, adoptando una perspectiva más amplia y comprendiendo que hay otras formas, y tal vez mejores, de realizar las cosas.
- Mejora Continua: el Benchmarking es un proceso continuo de gestión y auto-mejora.

Existen varios tipos de Benchmarking:

Interno (utilizándonos a nosotros mismos como base de partida para compararnos con otros), Competitivo (estudiando lo que la competencia hace y cómo lo hace), Fuera del sector (descubriendo formas más creativas de hacer las cosas), Funcional (comparando una función determinada entre dos o más empresas) y de Procesos de Negocio (centrándose en la mejora de los procesos críticos de negocio).

4.6.2 La reingeniería de procesos

La reingeniería de procesos es una técnica a partir de la cual se analiza en profundidad el funcionamiento de uno o varios procesos dentro de una empresa con el fin de rediseñarlos por completo y mejorar radicalmente.

La reingeniería de procesos surge como respuesta a las ineficiencias propias de la organización funcional en las empresas y sigue un método estructurado consistente en:

- Identificar los procesos clave de la empresa.
- Asignar responsabilidad sobre dichos procesos a un "propietario".
- Definir los límites del proceso.
- Medir el funcionamiento del proceso.
- Rediseñar el proceso para mejorar su funcionamiento.

Un proceso es un conjunto de actividades organizadas para conseguir un fin, desde la producción de un objeto o prestación de un servicio hasta la realización de cualquier actividad interna.

Durante muchos años, casi todas las organizaciones empresariales se han organizado verticalmente, por funciones. Actualmente, la organización por procesos permite prestar más atención a la satisfacción del cliente, mediante una gestión integral eficaz y eficiente: se produce la transición del sistema de gestión funcional al sistema de gestión por procesos.

CAPÍTULO 5: EL ÁREA DE LA CALIDAD INFORMÁTICA

5. EL ÁREA DE CALIDAD INFORMÁTICA

5.1 INSERCIÓN EN LA ESTRUCTURA DE LA EMPRESA:

5.1.1 Dependencia

La calidad comienza con una decisión estratégica que sólo puede ser tomada por la alta gerencia, la cual, es la decisión de competir como una compañía de categoría mundial. La calidad se concentra en lograr un desempeño de alta calidad en cada una de las facetas de la empresa.

La estrategia corporativa es la pauta de decisiones que adopta una compañía para determinar, configurar y revelar sus objetivos, metas o propósitos, elaborar políticas y los planes principales para lograr esas metas y definir los negocios en los que la compañía desea participar, el tipo de organización económica humana que pretende ser el carácter de la aportación económica y de otra índole que intenta hacer beneficio de sus accionistas, empleados, clientes y comunidades.

Aun cuando el proceso de formulación e implementación puede requerir las aportaciones del personal, la decisión final es en esencia una tarea del presidente del consejo administrativo o máximo funcionario ejecutivo.

La forma más fácil de entender el papel tan decisivo que desempeña la calidad en la planificación estratégica consiste en examinar los elementos que constituyen una estrategia:

- Misión
- Alcance del producto y el mercado
- Ventaja competitiva (diferenciación)
- Políticas de soporte
- Objetivos
- Cultura de la organización

La idea de que la calidad es esencial en todas las funciones de la empresa y no sólo en la manufactura, es fundamental. Esto se justifica por la necesidad de ofrecer una producción de calidad a los clientes internos y externos y de instaurar en toda la organización una cultura y un sistema de valores basados en la calidad. La relación entre calidad, rentabilidad y participación en el mercado se ha estudiado y se ha llegado a las siguientes conclusiones inequívocas:

- Un factor rige la participación en el mercado por encima de todos los demás: la calidad. Además, cuando se cuenta tanto con una calidad superior como con una fuerte participación en el mercado, la rentabilidad está prácticamente garantizada.
- La participación de la Dirección es fundamental ya que de esta depende que todo marche correctamente y de que los objetivos y metas se logren.
- No hay la menor duda de que la calidad relativa percibida y la rentabilidad tienen íntima relación entre sí. Ya sea que las ganancias se midan en términos de rendimiento sobre ventas o rendimiento sobre la inversión, las empresas que ostentan una oferta superior de producto o servicio superan con claridad a las que ofrecen una calidad inferior.

Es muy importante el liderazgo, debido a que bajo un buen líder siempre existirán excelentes trabajadores, los cuales a su vez llegarán a tener un compromiso tal con la empresa que todo mejorará. "Detrás de un buen líder no hay malos trabajadores".

5.2 SU COMPOSICIÓN

5.2.1 Jefatura

El compromiso y la participación de la alta gerencia tienen que ser explícitos y visibles. Muchos gerentes envían señales diciendo que darán apoyo a la calidad aunque esto signifique que cancelará todos los cursos destinados a elevar la calidad. Otros piensan que el problema de la calidad es de los trabajadores, desgraciadamente al cancelar cursos y no otorgar incentivos para los empleados provoca un gran descontento por parte del trabajador hacia la propia empresa.

El gerente tiene que tener un conocimiento de todo aquel que labore en la empresa y una comunicación personalizada, para evitar malos entendidos y sobre todo que la información se vaya distorsionando. Otro factor importante es que cada gerente tiene que convencer a quien no lo esté que la calidad y el compromiso hacia su empresa es lo más importante para poder dar un servicio y productos de calidad.

5.2.2 Integrantes

La empresa típica opera con una estructura de organización funcional y vertical, basada en relaciones de mando, procedimientos presupuestarios y clasificaciones de puestos muy específicas y detalladas. La división en departamentos se realiza de acuerdo con las funciones y tanto la comunicación como las recompensas y las lealtades tienen una orientación funcional. Se obliga a los procesos a fluir en sentido vertical y desde arriba hacia abajo, lo cual crea costosas barreras que impiden el libre flujo de los mismos.

El enfoque de sistemas aplicado a la forma de organizarse sugiere tres cambios significativos, uno de ellos conceptual y los otros que requieren un reordenamiento de la organización:

- El concepto del organigrama invertido.
- Un sistema de calidad interna en las distintas partes de la compañía.
- La integración horizontal y vertical de las funciones y actividades.

UN ORGANIGRAMA INVERTIDO

Es una pirámide simétrica en cuyo vértice se encuentra el presidente del consejo de administración y a partir de allí, la autoridad desciende en cascada por los siguientes niveles, hasta llegar a las funciones que están cerca de la base de la pirámide. Rara vez aparecen en el organigrama los supervisores de línea frontal y el personal que no llega a la categoría de supervisor casi nunca figura en él

¿Dónde están el supervisor y el empleado? Ellos son los que ponen la calidad de la firma en manos del cliente. Frente a la mirada de éste, esas personas son la compañía.

Es preciso invertir en el diagrama organizacional y colocar al cliente en el vértice superior, seguido de los empleados y los supervisores de línea frontal. Ellos son los que transmiten directamente la calidad. En este concepto no se modifica ni la jerarquía ni el flujo de la autoridad, pero el jefe ya no lo es en la acepción anticuada de la palabra. Ahora es un facilitador, un entrenador y un integrador, cuya tarea consiste en suprimir las barreras que impiden a sus subordinados llevar a feliz término su trabajo. Ese mismo papel recae ahora en la gerencia de nivel medio y alto. La calidad es hoy la responsabilidad de todos y no sólo del departamento a cargo de la verificación de la calidad.

5.2.3 Perfiles

Conocimientos generales.

Todo tipo de conocimientos tecnológicos, de forma actualizada y especializada respecto a las plataformas existentes en la organización.

Normas estándares para la auditoría interna.

Políticas organizacionales sobre la información y las tecnologías de la información.

Características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, compensaciones monetarias a los empleados, extensión de la presión laboral sobre los empleados, historia de la organización, cambios recientes en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, etc.

Herramientas de control y verificación de la seguridad.

Herramientas de monitoreo de actividades, etc.

Técnicas de Evaluación de riesgos.

Muestreo.

Cálculo pos operación.

Monitoreo de actividades.

Recopilación de grandes cantidades de información.

Verificación de desviaciones en el comportamiento de la data.

Análisis e interpretación de la evidencia, etc.

5.3 FUNCIONES Y RESPONSABILIDADES

5.3.1 Descripción

A través del liderazgo y diversas acciones, el comité ejecutivo proveerá los cometidos a desarrollar, implementar y mejorar en las capacidades de gestión de servicios dentro del contexto de la organización del negocio y los requisitos de clientes.

La gestión debe:

- Establecer las políticas de la gestión de servicios así como sus objetivos y planificaciones;
- Comunicar la importancia de conocer los objetivos de la gestión de servicios y la necesidad de la continua mejora;

- Asegurar que los requerimientos del cliente están fijados y comprendidos con el propósito de mejorar la satisfacción del cliente;
- Designar un miembro responsabilizado en la coordinación y gestión de todos los servicios;
- Determinar y proveer recursos para la planificación, implementación, monitorización, revisión y mejora en la entrega de los servicios y en la gestión, i.e. contratar personal apropiado, gestionar el movimiento de personal;
- Gestionar los riesgos de la gestión de los servicios de la organización;
- Llevar a cabo revisiones en la gestión de servicios, en los intervalos previstos, para asegurar la continuación de la idoneidad, la adecuación y la efectividad.

Las competencias del personal y la formación necesitan ser revisadas y gestionadas para posibilitar llevar a cabo los roles de forma efectiva.

La alta gestión deberá asegurar que sus empleados están concienciados de la relevancia e importancia de sus actividades y como deben contribuir a la consecución de los objetivos de la gestión de servicios.

Funciones a realizar:

- Concienciar a empresarios y trabajadores sobre la importancia de la calidad
- Iniciar el concepto de calidad con principios sencillos y prácticos
- Mejorar la calidad
- Aprovechar al máximo los recursos existentes
- Sensibilizar a la organización para el proceso de producción
- Unificar los elementos de la organización
- Fomentar la capacitación y mantenimiento
- Utilizar al operativo como elemento fundamental para mejorar la calidad
- Convencer sobre los beneficios de la calidad para que se piense en ella, no como un gasto
- Encontrar medios útiles y accesibles a la empresa para mejorar la calidad.

CAPÍTULO 6: INFRAESTRUCTURA DE LA CALIDAD

6. INFRAESTRUCTURA DE LA CALIDAD

En 1957 se funda en Europa la Organización Europea para la Calidad (EOQ). En 1988 se crea la Fundación Europea para la Gestión de la Calidad (EFQM) con el objetivo de promocionar la Gestión Total de la Calidad. Los organismos más importantes en Europa son:

1. Organismos de Normalización:
   - CEN (Comité europeo de normalización),
   - CENELEC (Comité europeo de normalización electrotécnica) y
   - ETSI (Instituto europeo de normas de telecomunicación).
2. Organismos de Acreditación Europea (EA)
3. Organismo de Control y Certificación (EOTC)
4. Organismo de Metrología (EUROMET)

Infraestructura de la calidad en España (MINER):

El Ministerio de Industria, Turismo y Comercio (MINER) es el encargado de revisar y adaptar la infraestructura para la calidad y la seguridad industrial. Esta infraestructura puede estar constituida por:

1. Organismos de normalización
2. Entidades de acreditación (ENAC en España):
   - Certificación y registro:
     - Certificación de sistemas de gestión, Certificación de Productos, Certificación de Servicios y Certificación de Personas.
   - Laboratorios de Ensayo.
   - Laboratorios de calibración.
   - Entidades Auditoras y de Inspección.

Promoción de la Calidad en España:

1. Plan Nacional de Calidad
2. Iniciativas de promoción (ATYCA)
3. Premio Príncipe Felipe a la Excelencia Empresarial

CAPÍTULO 7: CALIDAD, SEGURIDAD Y AUDITORÍA

7. CALIDAD, SEGURIDAD Y AUDITORÍA

7.1 INTRODUCCIÓN HISTÓRICA

Existe la evidencia de que alguna especie de auditoría se practicó en tiempos remotos. El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrolló el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley "Un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude". También reconocía... "Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas".

Desde 1862 hasta 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. En Inglaterra se siguió haciendo hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoría.

En los que podría llamarse los días en los que se formó la auditoría, a los estudiantes se les enseñaban que los objetivos primordiales de ésta eran:

- La detección y prevención de fraude.
- La detección y prevención de errores; sin embargo, en los años siguientes hubo un cambio decisivo en la demanda y el servicio, y los propósitos actuales son:
- El cerciorarse de la condición financiera actual y de las ganancias de una empresa.
- La detección y prevención de fraude, siendo éste un objetivo menor.

Este cambio en el objetivo de la auditoría continuó desarrollándose, no sin oposición, hasta aproximadamente 1940. En este tiempo "Existía un cierto grado de acuerdo en que el auditor podía y debería no ocuparse primordialmente de la detección de fraude".

El objetivo primordial de una auditoría independiente debe ser la revisión de la posición financiera y de los resultados de operación como se indica en los estados financieros del cliente, de manera que pueda ofrecerse una opinión sobre la adecuación de estas presentaciones a las partes interesadas.

Paralelamente al crecimiento de la auditoría independiente en los Estados Unidos, se desarrollaba la auditoría interna y del Gobierno lo que entró a formar parte del campo de la auditoría.

A medida que los auditores independientes se apercibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los departamentos de auditoría dentro de las organizaciones de los clientes, que se encargaría del desarrollo y mantenimiento de unos buenos procedimientos del control interno, independientemente del departamento de contabilidad general.

Progresivamente, las compañías adoptaron la expansión de las actividades del departamento de auditoría interna hacia áreas que están más allá del alcance de los sistemas contables. En nuestros días, los departamentos de auditoría interna son revisiones de todas las fases de las corporaciones, de las que las operaciones financieras forman parte.

La auditoría gubernamental fue oficialmente reconocida en 1921 cuando el Congreso de los Estados Unidos estableció la Oficina General de contabilidad.

Es compresible que si hablamos de una evolución histórica de la auditoría esta tenga que ver con la parte financiera de las entidades. Esto es debido a que el término en cuestión aparece bastante antes de la aparición de la informática.

Con lo anteriormente mencionado sólo se pretende tener una visión general de la evolución de la auditoría.

7.2 DEFINICIÓN

El concepto de auditoría se ha empleado con frecuencia incorrectamente puesto que se ha considerado como una evolución en la que cuyo único fin es detectar errores y señalar fallos.

El concepto de auditoría es mucho más que esto, es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

La palabra auditoría proviene del latín "*auditorius*", de ésta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Por otro lado, en el diccionario Español Sopena lo define como un revisor de cuentas colegiado. En un principio ésta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y la eficacia.

Podemos decir que la auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo son de carácter indudable.

De lo anteriormente citado, podemos decir que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallos en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y la eficiencia de una entidad.

7.2.1 Alcance y objetivos de la auditoría

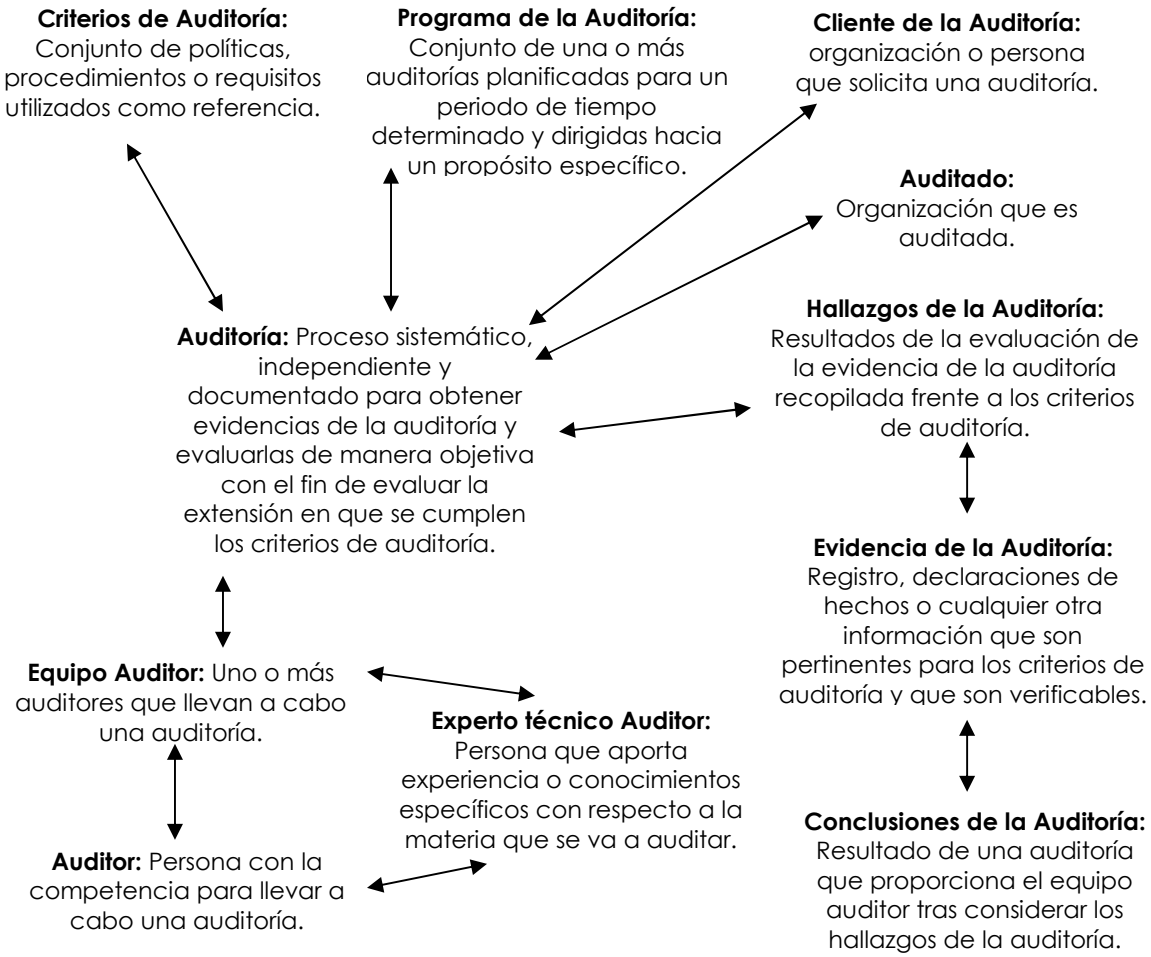
El alcance de la auditoría es asesorar a la gerencia con el propósito de:

- Delegar efectivamente las funciones.
- Mantener un adecuado control sobre la organización.
- Reducir a niveles mínimos el riesgo inherente.
- Revisar y evaluar cualquier fase de la actividad de la organización, contable, financiera, administrativa, operativa.

Los principales objetivos que constituyen la auditoría informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos.

Podemos clasificar los objetivos de la siguiente manera:

- Generales: dichos objetivos se basan en:
  - Velar por el cumplimiento de los controles internos establecidos.
  - Revisión de las cuentas desde el punto de vista contable, financiero, administrativo y operativo.
  - Ser un asesor de la organización.
- Específicos: los cuales se fundamentan en:
  - Revisar y evaluar la efectividad, propiedad y aplicación de los controles internos.
  - Cerciorarse del grado de cumplimiento de las normas, políticas y procedimientos vigentes.
  - Comprobar el grado de confiabilidad de la información que produzca la organización.
  - Evaluar la calidad del desempeño en el cumplimiento de las responsabilidades asignadas.
  - Promover la eficiencia operacional.



Esquema 1: Alcance de la Auditoría

7.2.2 Objetivo fundamental de la auditoría informática

La Auditoría Informática la podemos definir como el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales prefijadas en la organización.

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

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

La Auditoría del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

En un principio se tratará de todo lo relacionado con la seguridad, luego posteriormente todo aquello relacionado con la eficacia y terminar con la evaluación del sistema informático.

Los aspectos relativos al control de la **Seguridad de la Información** tienen tres líneas básicas en la auditoría del sistema de información:

- *Aspectos generales relativos a la seguridad.* En este grupo de aspectos habría que considerar, entre otros: la seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, atmósferas agresivas, agresiones y posibles sabotajes, seguridad físicas de las instalaciones, del personal informático, etc.
- *Aspectos relativos a la confidencialidad y seguridad de la información.* Estos aspectos se refieren no sólo a la protección del material, el logicial, los soportes de la información, sino también al control de acceso a la propia información (a toda o a parte de ella, con la posibilidad de introducir modificaciones en la misma).
- *Aspectos jurídicos y económicos relativos a la seguridad de la información.* En este grupo de aspectos se trata de analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho a la intimidad y el derecho a la información, y controlar los cada vez más frecuentes delitos informáticos que se cometen en la empresa. La propia evolución de las tecnologías de la información y su cada vez más amplia aplicación en la empresa, ha propiciado la aparición de estos delitos informáticos. En general, estos delitos pueden integrarse en dos grandes grupos: delitos contra el sistema informático y delitos cometidos por medio del sistema informático. En el primer grupo se insertan figuras delictivas tipificadas en cualquier código penal, como hurto, robo, revelación de secretos, etc..., y otro conjunto de delitos que ya no es tan frecuente encontrar, al menos con carácter general, perfectamente tipificados, como el denominado hurto de tiempo, destrucción de logiciales y datos, delitos contra la propiedad (material, terminales, cintas magnéticas,...). En el conjunto de delitos informáticos cometido por medio de sistemas informáticos cabría señalar, siempre con carácter doloso,

manipulaciones fraudulentas de logiciales, informaciones contenidas en bases de datos, falsificaciones, estafas, etc.

Merece la pena por su frecuencia y la dificultad de prueba el llamado hurto de uso. Este delito suele producirse cuando se utilizan los equipos informáticos de una organización para fines privados (trabajos externos, simple diversión,...). Los prejuicios, sobre todo económicos, que para la empresa puede significar esta modalidad de hurto de tiempo máquina, pueden ser cuantiosos, sobre todo cuando en el mismo interviene además el elemento comunicaciones. Se trata, en definitiva, de la utilización de unos equipos si tener derecho a ello o para un uso distinto del autorizado, y en el que lo lesionado no es la propiedad, sino una de las facultadas inherentes a la misma.

De la misma manera, a través de la auditoría del sistema de información será necesario controlar el adecuado equilibrio entre riesgos y costes de seguridad y la eficacia del propio sistema.

En cuanto a la **Eficacia del Sistema**, esta vendrá determinada, básicamente, por la aportación a la empresa de una información válida, exacta, completa, actualizada y oportuna que ayude a la adopción de decisiones, y todo ello medido en términos de calidad, plazo y coste. Sin el adecuado control, mediante la realización de auditorías al sistema de información, esos objetivos serían difíciles de conseguir, con la siguiente repercusión en una adecuada dirección y gestión en la empresa.

Uno de los aspectos más significativos de la Auditoría Informática se refiere a los datos relativos a la **Rentabilidad del Sistema,** homogeneizados en unidades económicas de cuenta. La rentabilidad del sistema debe ser medida mediante el análisis de tres valores fundamentales: la evaluación de los costes actuales, la comparación de esos costes actuales con magnitudes representativas de la organización, y la comparación de los costes del sistema de información de la empresa con los de empresas similares, preferentemente del mismo sector de actividad.

Cómo evaluar de forma concreta estos tres aspectos fundamentales, que conforman la rentabilidad del sistema de información, es lo que se analiza seguidamente.

- *Evaluación de los costes actuales*. Conocer, en términos económicos, los costes que para una empresa supone su sistema de información, constituye uno de los aspectos básicos de la auditoría informática. Se trata de cuantificar los costes de los distintos elementos que configuran el sistema de información y que en términos generales son los siguientes:
- *Hardware*. Se trata de analizar la evolución histórica del hardware en la empresa, justificando dicha evolución. Es importante conocer el coste del material (unidad central, periféricos, soporte,...) durante los últimos cinco años. También será necesario analizar la utilización de cada elemento hardware de la configuración, cifrándola en horas/mes, asegurando que la configuración utilizada se corresponde con el menor valor utilización/coste, y examinar la coherencia del mismo.
- *Software*. Análisis de los costes relativos al sistema lógico, tanto en sus aspectos relativos a la explotación (adecuación del sistema operativo, versión del software utilizado,...) como en los aspectos relativos a la programación de las distintas aplicaciones (prioridades de ejecución, lenguaje utilizado...).

- *Capturas de datos*. Análisis de los costes relativos a la captura de datos, de las fuentes de información, tanto internas como externas de la empresa.
- *Grabación de datos*. Es necesario conocer también los costes relativos a la trascripción de datos en los soportes adecuados (costes de personal, equipos y máquinas auxiliares).
- *Explotación*. Análisis de los costes imputados a los factores relativos a la explotación en sentido amplio (tratamiento manual, tiempos de realización de aplicaciones, tiempo de respuesta, control errores, etc.).
- *Aplicaciones*. Se trata de evaluar los costes del análisis funcional, el análisis orgánico, la programación, las pruebas de programas, preparación de datos y costes de desarrollo de cada aplicación medido en horas.
- *Personal*. Teniendo en cuenta el nivel cualitativo y cuantitativo (las distintas categorías, equilibrio entre esas categorías, remuneraciones salariales, horas extraordinarias), se trata de analizar los costes de personal directamente relacionado con el sistema de información. En este apartado deberán tenerse en cuenta también los costes relativos a la formación del personal.
- *Documentación*. Es necesario no sólo verificar que la documentación relativa al sistema de información sea clara, precisa, actualizada y completa, sino también los costes relativos a su elaboración y actualización.
- *Difusión de la información.* Se trata de evaluar los costes de difundir la información, es decir, hacer llegar a los usuarios del sistema la información demandada o aquella considerada necesaria en los distintos niveles de la organización. Se trata, en definitiva, de conocer y analizar los costes que para la empresa supone disponer del sistema de información.
- *Comparación de los costes actuales con magnitudes representativas de la organización.* No es suficiente conocer los costes totales del sistema de información; es necesario, además, comparar este coste con magnitudes representativas de la empresa. Se trata de conocer los porcentajes que en relación con el coste total son imputables al *hardware,* al *software,* a la captura de datos, grabación, explotación, aplicaciones, suministros, mantenimiento, personal, documentación y difusión de la información. Conocer la relación de costes/ ahorro/productividad del personal (analistas, programadores, operadores, auxiliares, etc.) y analizar la evolución del coste de la hora útil de la memoria central. Pero ese análisis de costes adquiere su especial significado cuando éstos se relacionan con magnitudes representativas de la empresa, por ejemplo: la cifra de negocios, la cifra de ventas, etc. El dato de costes del sistema y su comparación con otras magnitudes constituye una valiosa información que deberá ser especificada en las conclusiones de la auditoría informática y que tendrá una notable incidencia respecto a los planteamientos de futuro del sistema de información.
- *Comparación de los costes del sistema de información de la empresa con los de empresas similares.* El análisis de costes y su comparación con otras magnitudes representativas, debe completarse, siempre que ello sea posible, con los costes de los sistemas de información de empresas similares a la que es objeto de auditoría. Es imprescindible conocer los costes que representan la obtención, tratamiento y difusión

de la información en la empresa. La información es un recurso de la empresa y por lo tanto un activo de la misma. De ahí la importancia de poder disponer de una comparación de los costes del sistema de información con los de otras empresas. Esa comparación debe realizarse con empresas del mismo sector. Ello permite comparar el nivel de costes del sistema de información de la empresa auditada con la media del sector. Los tres aspectos analizados en relación con los costes aportarán una importante información que permitirá adoptar correctas decisiones, a partir de la auditoría realizada sobre el sistema de información de la empresa.

7.2.3 Actividades a ser realizadas en una auditoría

Reunión Inicial.

Debe darse una reunión de apertura. El propósito de una reunión de apertura es el de:

- Presentar a los miembros del equipo auditor a la gerencia del auditado.
- Revisar el alcance, los objetivos y el plan de auditoría y llegar a un acuerdo con respecto a la tabla de tiempos de la auditoría.
- Proveer un resumen corto de la metodología y de los procedimientos a ser utilizados durante la auditoría.
- Confirmar que los recursos y facilidades necesitadas por el equipo auditor estén disponibles.
- Promover la participación activa del auditado.
- Revisar los procedimientos de seguridad y emergencia relevantes del local para el equipo auditor.

Detección de Evidencia

La información apropiada debe ser recopilada, analizada, interpretada y documentada para ser utilizada como evidencia de la auditoría en un proceso de verificación y evaluación para determinar si los criterios de la auditoría se están cumpliendo.

La evidencia de la auditoría debe ser de tal calidad y cantidad que auditores de calidad competentes, trabajando independientemente cada uno, lleguen a resultados de auditoría similares a la evaluación de la misma evidencia contra los mismos criterios de auditoría.

La evidencia de la auditoría debe ser recolectada por medio de entrevistas, revisión de documentos y la observación de actividades y condiciones.

La información recopilada por medio de entrevistas debe ser verificada por medio de la adquisición de información de respaldo de fuentes independientes, como observaciones, registros y resultados de medidas existentes. Declaraciones que no puedan ser confirmadas deben ser identificadas como tales.

Los auditores deben examinar la base de programas de muestreo relevantes y los procedimientos para asegurar un control de calidad de los procesos de muestreo y medición efectivos.

Resultados de la Auditoría

El equipo auditor debe revisar toda la evidencia de la auditoría para determinar dónde no se cumple con los criterios de auditoría del SGC. El equipo auditor debe entonces asegurarse que los resultados de la auditoría de no conformidad sean documentados de forma clara, concisa y que sean respaldados por la evidencia de la auditoría.

La evidencia contrastada durante la auditoría de calidad inevitablemente será solamente una muestra de la información disponible, parcialmente debido al hecho de que una auditoría de calidad sea realizada durante un periodo de tiempo limitado y con recursos limitados. Por lo tanto existe un elemento de incertidumbre inherente a todas las auditorías de calidad y a todos los usuarios de los resultados, todas las auditorías de calidad deben estar seguras de la recopilación de las evidencias y no conformidades siendo contrastada su evidencia física y documental.

El auditor de calidad debe considerar las limitaciones asociadas con la evidencia de la auditoría constatada durante ésta y el reconocimiento de la fiabilidad en los resultados y cualquier conclusión de la auditoría, se deben tomar estos factores en cuenta al planear y ejecutar la auditoría.

El auditor de calidad debe obtener suficientes evidencias para que los resultados individuales de la auditoría, agregados a los resultados de menor significado, puedan afectar cualquier conclusión alcanzada.

Los resultados de la auditoría deben ser revisados con la gerencia del auditado con el fin de obtener el reconocimiento de la base de todos los resultados de no conformidad.

Reunión final

Luego de completar la fase de recopilación de evidencia y antes de preparar un informe de la auditoría, los auditores deberán tener una reunión con la gerencia del auditado y aquellos responsables de las funciones auditadas. El propósito principal de esta reunión es el de presentar los resultados de la auditoría al auditado, de tal manera que se tenga una comprensión y reconocimiento claro de la base de dichos resultados.

Los desacuerdos deben ser resueltos, si es posible antes de que el auditor líder presente el informe, las discusiones finales en el significado y descripción de los resultados de la auditoría última recaen en el auditor líder, sin embargo el cliente puede todavía estar en desacuerdo con los resultados.

Actividades Posteriores al Trabajo en la Empresa.

Informe.

Los resultados de la auditoría o un resumen de estos deben ser comunicados al cliente en un informe escrito.

El informe escrito se prepara bajo la dirección del auditor líder, quien es el responsable de su exactitud y perfección. Las informaciones que se tomen en el informe de la auditoría deben ser los predeterminados en el plan de la auditoría.

La información relativa a la auditoría que se debe incluir en el informe debe incluir, pero no está limitada a:

- La identificación de la organización auditada y del cliente.
- Los objetivos y alcance acordados de la auditoría.
- Los criterios acordados contra los que se realizó la auditoría.
- El período cubierto por la auditoría.
- La(s) fecha(s) en que la auditoría fue realizada.
- La identificación del equipo auditor.
- La identificación de los representantes del auditado que participaron en la auditoría.
- Un resumen del proceso de auditoría, incluyendo cualquier obstáculo enfrentado.
- Las conclusiones de la auditoría.
- Las declaraciones de confidencialidad de los contenidos.
- La lista de distribución del informe de la auditoría.

7.2.4 Su relación con el área de calidad informática

La calidad es imprescindible en la fase de desarrollo de un sistema auditor, ya que ofrece la seguridad razonable de que el departamento de auditoría mantiene la capacidad para efectuar de forma eficiente y eficaz sus funciones, y así alcanzar un alto nivel de credibilidad y confianza ante la dirección, auditores y sociedad. Se pueden entrar a analizar varios parámetros que deben ser considerados en la calidad de la auditoría.

Los auditados deben percibir que el grupo de auditores trabaja para que las cosas funcionen bien y no como un servicio de control e inspección. La calidad no se improvisa por lo que su sistematicidad es un requisito indispensable; esto requiere de un grupo de exigencias agrupadas en: Supervisión del trabajo, Revisión Interna y Revisión Externa.

La preocupación y ocupación por la calidad es un objeto inaplazable y ésta no sólo, concierne a los productos o servicios, sino a toda la vida y actividad de la empresa. Fallas en la calidad afectan a toda la organización y la auditoría inmersa en el análisis de estas organizaciones debe tener calidad y crear un clima de confiabilidad hacia los auditores conociendo de antemano que la calidad no se improvisa sino que es fruto de su trabajo, competente, honesto, riguroso y sistemático.

7.3 ÁMBITO DE ACTUACIÓN

7.3.1 Respecto a las áreas informáticas

Organizaciones de todo tipo pueden tener la necesidad de demostrar su responsabilidad con el sistema de gestión de calidad implantado (SGC) y la práctica asociada de Auditoría de calidad se ha tornado como una forma de satisfacer esta necesidad. La intención de estos sistemas es la de ayudar a una organización a establecer y mejorar sus políticas, objetivos, estándares y otros requerimientos de calidad.

Un conjunto de estándares de calidad han sido elaborados para guiar a las organizaciones, auditores y sus clientes, en los principios comunes para la ejecución de auditorías de calidad. Éstas también proveen definiciones de auditoría de calidad y otros términos relacionados.

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar.

Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto, planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

Objetivos a corto y largo plazo

Recursos y materiales técnicos:

- Solicitar documentos sobre los equipos, número de ellos, localización y características.
- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados).
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos. Sistemas.
- Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.
- Manual de normas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

- No se tiene y se necesita.
- No se tiene y no se necesita.
- No se tiene pero es necesaria.

Se tiene la información:

- No se usa
- Es incompleta.
- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento).
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

7.3.2 En el entorno informático

Por la creciente complejidad de los entornos, cada vez tienen mayores y peores consecuencias los delitos, los fraudes, los desastres e incidencias y los más probables de todos: los errores y omisiones.

Por otra parte, cada día es más necesario optimizar la gestión de los recursos informáticos y tecnológicos en general, entendiendo como tales: los propios recursos humanos, los equipos y las comunicaciones, los paquetes y las aplicaciones.

Los entornos son cada día más complejos, con redes de comunicaciones y terminales (a menudo ordenadores personales con emulación), bases de datos distribuidas, sistemas de información a la Alta Dirección (EIS) y de soporte a las decisiones (DSS), comercio electrónico, acceso desde dispositivos móviles, y la aparición de tendencias y tecnologías que incrementan las posibilidades a la vez que los riesgos.

La auditoría informática comprende el entorno informático de una entidad, abarcando todas o algunas de sus áreas, como equipos, sistemas operativos y paquetes, aplicaciones y el proceso de su desarrollo, organización y funciones, las comunicaciones, la propia gestión de los recursos informáticos...

El ámbito ha de quedar perfectamente definido, especialmente en entidades grandes y dispersas, y en cuanto a las áreas por centro: desarrollo, producción....

La auditoría informática puede cubrir muchos aspectos, que vendrán determinados por el objetivo de la auditoría (interna o externa).

Habitualmente un proceso de auditoría abarca varios de los siguientes aspectos:

- Verificación de controles en general: Evaluación del sistema de control interno.
- De cumplimiento: de políticas, estándares y procedimientos de la propia entidad, de normas legales aplicables, de contratos...
- De seguridad, de calidad: (seguridad física y/o lógica).
- Operativa, de gestión (eficiencia / eficacia): Se debe distinguir entre auditoría operativa (que puede limitarse a revisión de procedimientos operativos y de operaciones en general) y propiamente auditoría de gestión, que pudiendo incluir lo anterior, ha de referirse también al análisis y revisión de "ratios" y estándares de gestión, al cumplimiento de planes y objetivos. En relación con ellas podríamos hablar de auditorías de eficiencia y eficacia).
- Apoyo auditoría de Cuentas: La auditoría informática puede servir de apoyo a la auditoría de cuentas, garantizando que el proceso de los datos (a lo largo de todo su ciclo de vida) y las aplicaciones / paquetes que los manejan son los adecuados, y están razonablemente exentos de error y de fraude.
- Relacionadas con los recursos humanos: (Personas).
- Especiales (fusiones / absorciones).
- De reglamento de desarrollo de LOPD.

7.4 SÍNTOMAS DE AUDITORÍA

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

- Síntomas de descoordinación y desorganización:
  - No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.
  - Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

  (Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante).

- Síntomas de mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
  - No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financiero:
  - Incremento desmesurado de costes.
  - Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  - Desviaciones Presupuestarias significativas.
  - Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

- Síntomas de Inseguridad: Evaluación de nivel de riesgos.
  - Seguridad Lógica
  - Seguridad Física
  - Confidencialidad

(Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales).

  - Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia* Totales y Locales.
  - Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

**Planes de Contingencia:*

Por ejemplo, la empresa sufre un corte total de energía o explota, ¿Cómo sigo operando en otro lugar? Lo que generalmente se pide es que se hagan Backus de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro afuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono Telecom, a las oficinas paralelas, Telefónica. En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backus se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

7.5 TIPOS Y CLASES DE AUDITORÍAS

El departamento de Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. He aquí, la *Auditoría Informática de Usuario*. Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una *Auditoría Informática de Actividades Internas*.

El control del funcionamiento del departamento de informática con el exterior, con el usuario se realiza por medio de la Dirección. Su figura es importante, en tanto en cuanto es capaz de interpretar las necesidades de la Compañía. Una informática eficiente y eficaz requiere el apoyo continuado de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoría Informática de Dirección*. Estas tres auditorías, más la auditoría de Seguridad, son las cuatro Áreas Generales de la Auditoría Informática más importantes.

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Áreas Especificas de la Auditoría Informática más importantes.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Tabla 1: Áreas Específicas de la Auditoría Informática

Cada Área Especifica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

7.5.1 Auditoría de Explotación

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc.

La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales.

Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que sea necesario transformar, y que se sometan previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos.

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

**Batch y Tiempo Real:*

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no sólo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis:

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todas las líneas asociadas al Sistema. El Centro de Diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

7.5.2 Auditoría de Desarrollo

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Pre-requisitos del Usuario (único o plural) y del entorno.
- Análisis funcional.
- Diseño.
- Análisis orgánico (Pre-programación y Programación).
- Pruebas.
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. *Revisión de las metodologías utilizadas*: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. *Control Interno de las Aplicaciones*: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:
   - Estudio de Vialidad de la Aplicación. (Importante para Aplicaciones largas, complejas y caras).
   - Definición lógica de la Aplicación. (Se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto).
   - Desarrollo Técnico de la Aplicación. (Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles).
   - Diseño de Programas. (Deberán poseer la máxima sencillez, modularidad y economía de recursos).
   - Métodos de Pruebas. (Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales).
   - Documentación. (Cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación).
   - Equipo de Programación. (Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos).
3. *Satisfacción de usuarios:* Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

4. *Control de Procesos y Ejecuciones de Programas Críticos:* El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programas módulo no coincidieran se podría provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:
    1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso.
    2. Compile y monte ese Programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
    3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use la Aplicación como si la estuviera usando en Producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien").

Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan.

Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por todo.

7.5.3 Auditoría de Sistemas

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.

Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles

incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte del propio ordenador. Esto, por razones económicas y por razones de comprobación de que el ordenador podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

Software de Teleproceso (Tiempo Real):

No se incluye en Software Básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de Tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El Tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema
- De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los Sistemas y Subsistemas:

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de Tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización* fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

**Optimización:*

Por ejemplo: cuando se instala una Aplicación, normalmente está vacía, no

tiene nada cargado adentro. Lo que puede suceder es que, a medida que se va cargando, la Aplicación se va poniendo cada vez más lenta; porque todas las referencias a tablas es cada vez más grande, la información que está moviendo es cada vez mayor, entonces la Aplicación se tiende a poner lenta. Lo que se tiene que hacer es un análisis de performance, para luego optimizarla, mejorar el rendimiento de dicha Aplicación.

Administración de Base de Datos:

El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

La administración tendría que estar a cargo de Explotación. El auditor de Base de Datos debería asegurarse qué Explotación conoce suficientemente las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

7.5.4 Auditoría de Comunicaciones

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuántas líneas existen, cómo son y dónde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Ordenadores con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

7.5.5. Auditoría de Seguridad

El ordenador es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en los ordenadores personales, se ha dado otro factor que hay que considerar: el llamado "virus" de los ordenadores, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otros ordenadores, no exista la posibilidad de transmisión del virus. El uso inadecuado del ordenador comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de los ordenadores grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, qué usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Área General y como Área Específica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Específica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico.

Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal.
- Elementos técnicos y procedimientos.
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- El papel de los auditores, tanto internos como externos.
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan.

Las matrices de riesgo se representan en cuadros de doble entrada "Amenaza-Impacto", en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza -: Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

Tabla 2: Ejemplo de matriz de riesgo

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

7.6 REQUISITOS DE AUDITORÍA INFORMÁTICA

Los requisitos necesarios para realizar una auditoría informática son:

- Debe seguir una metodología preestablecida.
- Se realizará en una fecha precisa y fija.
- Será personal extraño al servicio de informática.

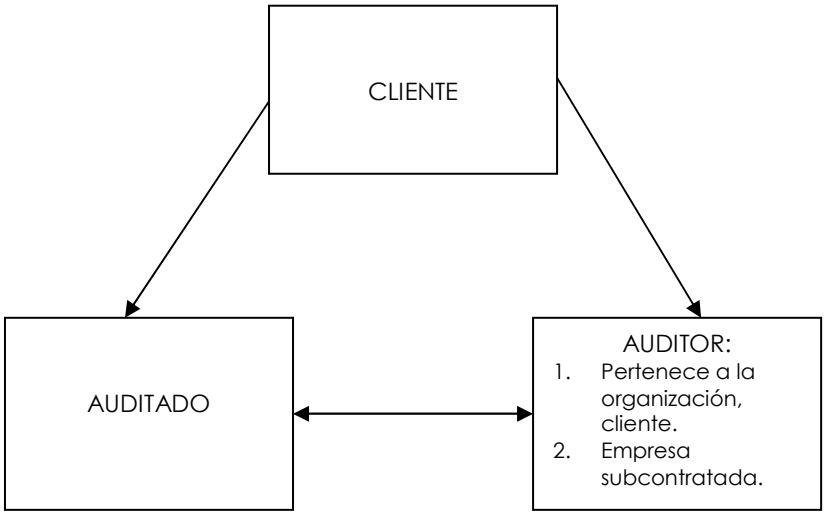
7.7 AUDITORÍA INTERNA Y/O EXTERNA

7.7.1 Externa: bases para la contratación

Los principales objetivos de la auditoría externa son:

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados.
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores.
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia.
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio.
- Control de las actividades de investigación y desarrollo.

7.7.1.1 Auditorías externas de calidad



Esquema 2: Auditorías externas de Calidad

- El cliente y el auditado no son la misma organización.
- El auditor en este caso no pertenece a la organización auditada, sino que proviene de la organización cliente o es una persona o grupo de personas subcontratadas, externas tanto al cliente como al auditado.

La decisión de iniciar la auditoría procede en este caso del cliente y debe ser aceptada por el suministrador que tiene. La empresa puede oponerse a someterse a dicha auditoría, pero entonces tiene que enfrentarse a las posibles consecuencias, como la posible ruptura de relaciones comerciales.

El cliente pude solicitar este tipo de auditoría por varios motivos:

- Auditoría de evaluación. Antes de comenzar una relación contractual con un suministrador, puede desear que se someta a una auditoría para hacer una evaluación del mismo.
- Auditoría de seguimiento. Dentro de un marco contractual, el cliente puede desear evaluar de forma periódica a su suministrador.
- Dentro del marco contractual, puede desearse evaluar al suministrador después, por ejemplo, de la implantación de un plan de acciones correctoras emprendido ante los resultados de una auditoría anterior.

En este marco la auditoría es una herramienta de mejora basada en un marco de colaboración entre cliente y suministrador.

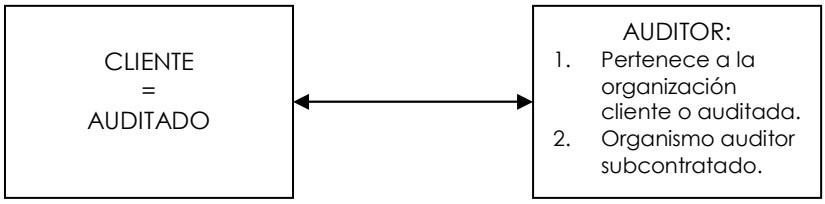
Los resultados de este tipo de auditorías deben permanecer en el marco de relaciones cliente / suministrador.

7.7.2 Interna: dependencia y funciones

Los principales objetivos de la auditoría interna son:

- Revisión y evaluación de controles contables, financieros y operativos.
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento.
- Custodia y contabilización de activos.
- Examen de la fiabilidad de datos.
- Divulgación de políticas y procedimientos establecidos.
- Información exacta de la gerencia.

7.7.2.1 Auditorías internas de calidad



Esquema 3: Auditorías internas de Calidad

- El cliente y el auditado son la misma organización. Es decir, es organizada por la propia empresa, en sus propias instalaciones. Aunque puede existir una petición del propio sector de la empresa o de otro sector para que se lleve a cabo.
- El auditor puede ser en este caso un miembro de la misma organización o una persona o grupo de personas subcontratadas, externas a la organización.

La auditoría interna de la calidad es la única herramienta de mejora impuesta por la norma UNE-ISO 9001:2008.

La auditoría interna es el medio de verificar que el sistema de la calidad implantado resulta apropiado y además supone una herramienta de mejora permanente en la empresa.

Los resultados de este tipo de auditorías se presentan al responsable del sector auditado, que extraerá las conclusiones oportunas de acuerdo con la dirección y con el cliente.

El análisis de resultados y las conclusiones de la auditoría son documentos internos de la empresa.

7.7.3 Diferencias entre auditoría interna y externa

CONCEPTO	AUDITORÍA INTERNA	AUDITORÍA EXTERNA
1)Sujeto	**Empleados**: evitar que traslade información a otros sitios	**Profesional independiente**: se fija sólo en la imagen fiel
2)Grados de independencia	**Limitada:** El auditor interno no se limita exclusivamente a dar un informe de todo sino que se dedica a evaluar las peticiones de la dirección o del consejo. ESTÁ OBLIGADO A SEGUIR UN PROGRAMA	**Total**: Está sujeto a las directrices técnicas de auditoría.
3) Responsabilidad	**Laboral**	**Penal**: El informe del auditor tiene consecuencias jurídicas
4) Objetivo	Examen de gestión	Examen de la situación para dar opinión.
5) Informe emitido	Dirigido a la gerencia, dirección y/o Consejo de Administración. Puede hacerse para cualquier tipo de empresa	Accionistas o Consejo de Administración: con carácter obligatorio si lo obliga la ley o con carácter optativo si lo desea la empresa.
6) Uso del Informe	Va dirigido exclusivamente a la empresa.	Va dirigido a la empresa y al público en general.

Tabla 3: Diferencias Auditoría externa/interna

7.8 REVISIÓN DE CONTROLES DE LA GESTIÓN INFORMÁTICA

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.

2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.
3. Los Procedimientos Específicos Informáticos. Igualmente, se revisará su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

7.9 PERFIL DEL AUDITOR INFORMÁTICO

7.9.1 Capacidad, conocimientos, formación

Entendemos por auditor a aquella persona profesional, que se dedica a trabajos de auditoría habitualmente con ejercicio de una ocupación técnica.

Para ordenar e imprimir cohesión a su labor, el auditor cuenta con un una serie de funciones tendientes a estudiar, analizar y diagnosticar la estructura y funcionamiento general de una organización.

Las funciones tipo del auditor son:

- Estudio de la normatividad, misión, objetivos, políticas estrategias, planes y programas de trabajo.
- Desarrollo del trabajo de una auditoría.
- Definición de los objetivos, alcance y metodología para instrumentar una auditoría
- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados.
- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo.
- Diagnostico sobre los métodos de operación y los sistemas de información.
- Detección de los hallazgos y evidencias e incorporarlos a los papeles de trabajo.
- Representación de las normas de actuación dictadas por los grupos de filiación, corporativos, sectoriales e instancias normativas y, en su caso, globalizadoras.
- Propuesta de los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización.
- Análisis de la estructura y funcionamiento de la organización en todos sus ámbitos y niveles.
- Revisión del flujo de datos y formas.
- Consideración de las variables ambientales y económicas que inciden en el funcionamiento de la organización.

- Mantenimiento del nivel de actuación a través de una interacción y revisión continúa de los avances.
- Diseño y preparación de los informes de una auditoría.

Los **conocimientos** que debe poseer un auditor deben ir acorde con el tipo de auditor que se trate, puesto que esto le permitirá interactuar de manera natural y congruente con los mecanismos de estudio que de una u otra manera se emplearán durante su desarrollo.

Atendiendo a estas necesidades es recomendable tener en cuenta los siguientes niveles de formación:

- Académica: estudios a nivel técnico, licenciatura o postgrado en administración, informática, comunicación, ciencias políticas, administración pública, relaciones industriales, ingeniería industrial, psicología, pedagogía, ingeniería en sistemas, contabilidad, derecho, relaciones internacionales y diseño gráfico.

  Otras especialidades como, matemáticas, ingeniería y arquitectura, pueden contemplarse siempre y cuando hayan recibido una captación que les permita intervenir en el estudio.

- Complementaria: instrucción en la materia, obtenida a lo largo de la vida profesional por medio de diplomas, seminarios, foros y cursos, entre otros.

- Empírica: conocimiento resultante de la implementación de auditorías en diferentes instituciones sin contar con un grado académico.

  Adicionalmente, deberá saber operar equipos de cómputo y de oficina, y dominar él ó los idiomas que sean parte de la dinámica de trabajo de la organización bajo examen. También tendrán que tener en cuenta y comprender el comportamiento organizacional cifrado en su cultura.

  Una actualización continua de los conocimientos permitirá al auditor adquirir la madurez de juicio necesaria para el ejercicio de su función en forma prudente y justa.

En forma complementaria a la formación profesional, teórica y/o práctica, el equipo auditor demanda de otro tipo de cualidades que son determinantes en su trabajo, referidas a recursos personales producto de su desenvolvimiento y dones intrínsecos a su carácter.

La expresión de estos atributos puede variar de acuerdo con el modo de ser y el deber ser de cada caso en particular, sin embargo es conveniente que, quien se dé a la tarea de cumplir con el papel de auditor, sea poseedor de las siguientes características:

- Actitud positiva.
- Estabilidad emocional.
- Objetividad.
- Sentido institucional.
- Saber escuchar.
- Creatividad.
- Respeto a las ideas de los demás.
- Mente analítica.
- Conciencia de los valores propios y de su entorno.

- Capacidad de negociación.
- Imaginación.
- Claridad de expresión verbal y escrita.
- Capacidad de observación.
- Iniciativa.
- Discreción.
- Facilidad para trabajar en grupo.
- Comportamiento ético.

Uno de los elementos fundamentales que se tiene que considerar en las características del equipo, es el relativo a su **experiencia** personal de sus integrantes, ya que de ello depende en gran medida el cuidado y diligencia profesionales que se emplean para determinar la profundidad de las observaciones.

Por la naturaleza de la función a desempeñar existen varios campos que se tienen que dominar:

- Conocimiento de las áreas sustantivas de la organización.
- Conocimiento de las áreas adjetivas de la organización.
- Conocimiento de esfuerzos anteriores
- Conocimiento de casos prácticos.
- Conocimiento derivado de la implementación de estudios organizacionales de otra naturaleza.
- Conocimiento personal basado en elementos diversos.

El equipo auditor debe realizar su trabajo utilizando toda su capacidad, inteligencia y criterio para determinar el alcance, estrategia y técnicas que habrá de aplicar en una auditoría, así como evaluar los resultados y presentar los informes correspondientes.

Para éste efecto, debe de poner especial cuidado en:

- Preservar la independencia mental.
- Realizar su trabajo sobre la base de conocimiento y capacidad profesional adquiridos.
- Cumplir con las normas o criterios que se le señalen.
- Capacitarse en forma continua.

También es necesario que se mantenga libre de impedimentos que resten credibilidad a sus juicios, por que debe preservar su autonomía e imparcialidad al participar en una auditoría.

Es conveniente señalar, que los impedimentos a los que normalmente se puede enfrentar son: personales y externos.

Los primeros, corresponden a circunstancias que recaen específicamente en el auditor y que por su naturaleza pueden afectar su desempeño, destacando las siguientes:

- Vínculos personales, profesionales, financieros u oficiales con la organización que se va a auditar.
- Interés económico personal en la auditoría.

- Corresponsabilidad en condiciones de funcionamiento incorrectas.
- Relación con instituciones que interactúan con la organización.
- Ventajas previas obtenidas en forma ilícita.

Los segundos están relacionados con factores que limitan al auditor a llevar a cabo su función de manera puntual y objetiva como son:

- Injerencia externa en la selección o aplicación de técnicas o metodología para la ejecución de la auditoría.
- Interferencia con los órganos internos de control.
- Recursos limitados para desvirtuar el alcance de la auditoría.
- Presión injustificada para propiciar errores inducidos.

En estos casos, tiene el deber de informar a la organización para que se tomen las providencias necesarias.

Finalmente, el equipo auditor no debe olvidar que la fortaleza de su función está sujeta a la medida en que afronte su compromiso con respeto y en apego a normas profesionales tales como:

- Objetividad.- Mantener una visión independiente de los hechos, evitando formular juicios o caer en omisiones, que alteren de alguna manera los resultados que obtenga.
- Responsabilidad.- Observar una conducta profesional, cumpliendo con sus encargos oportuna y eficientemente.
- Integridad.- Preservar sus valores por encima de las presiones.
- Confidencialidad.- Conservar en secreto la información y no utilizarla en beneficio propio o de intereses ajenos.
- Compromiso.- Tener presente sus obligaciones para consigo mismo y la organización para la que presta sus servicios.
- Equilibrio.- No perder la dimensión de la realidad y el significado de los hechos.
- Honestidad.- Aceptar su condición y tratar de dar su mejor esfuerzo con sus propios recursos, evitando aceptar compromisos o tratos de cualquier tipo.
- Institucionalidad.- No olvidar que su ética profesional lo obliga a respetar y obedecer a la organización a la que pertenece.
- Criterio.- Emplear su capacidad de discernimiento en forma equilibrada.
- Iniciativa.- Asumir una actitud y capacidad de respuesta ágil y efectiva.
- Imparcialidad.- No involucrarse en forma personal en los hechos, conservando su objetividad al margen de preferencias personales.
- Creatividad.- Ser positivo e innovador en el desarrollo de su trabajo.

7.10 REQUISITOS DE UNA AUDITORÍA DE CALIDAD

7.10.1 Plan de auditorías

El Plan de Auditorías debe estar incluido en el Plan Anual de la Calidad. En el Plan de Auditorías deben estar provistos los equipos que van a realizar las auditorías y su dependencia jerarquía, así como las funciones, las misiones y las

responsabilidades de los auditores.

En el proceso de Planificación de la Calidad hay que auditar todos los aspectos relacionados con la calidad, lo que exige tener:

- Una preparación adecuada.
- Una base objetiva para tomar decisiones.

Una preparación adecuada significa establecer:

- La norma con que se va a auditar.
- El sistema de evaluación previsto.
- La formación y aprobación de las normas y sistemas de los auditores y de los auditados.
- La forma de canalizar y de presentar los resultados.

Una base objetiva y eficaz para las auditorías se obtiene a través del conocimiento de hechos que han ocurrido en la empresa. Como por ejemplo:

- De los resultados de las homologaciones realizadas por los clientes.
- De las quejas y reclamaciones de los clientes.
- Del análisis de las actuaciones de los grupos de trabajo.
- De las acciones correctoras de anteriores auditorías.
- Del análisis y composición de los Costes Totales de la Calidad.

Con la preparación adecuada y la base objetiva, el Comité de la Calidad establece un calendario de fechas. Una vez realizadas las auditorías, el Comité de Calidad debe prever la formación de un grupo de trabajo que realice un seguimiento de las acciones correctoras de los planes de mejora.

7.10.2 Manual de las auditorías

Según los expertos, es aconsejable elaborar un Manual de Procedimientos de las Auditorías, con el objetivo de facilitar su funcionamiento. En el Manual se establecen los siguientes puntos:

- La introducción al Sistema de Auditorías de Calidad.
- Los objetivos de los Planes de Auditoría.
- La situación orgánica de los diferentes tipos de auditores (organización y competencias).
- El establecimiento de los diferentes sistemas a aplicar en los distintos tipos de Auditorías de la Calidad y de los niveles de Calidad aceptable.
- El muestreo: métodos para determinar el tamaño, la frecuencia y el modo de elección de las muestras.
- Las normas generales para la determinación de la criticidad de los diferentes parámetros.
- La metodología de recogida, de elaboración, y de presentación de los datos.
- Los preinformes, la forma de comunicación a los departamentos afectados, los informes y la metodología a seguir.
- Los Planes de Mejora y su encuadre en el grupo de trabajo de seguimiento.

- La frecuencia en la realización de las auditorías y la medición del avance.

El Plan Anual de Auditorías complementa al Manual de Auditorías ya que:

- Concreta las áreas a auditar.
- Establece el calendario de las áreas a auditar.
- Designa a la persona que auditará cada área.

Todo ello aprobado por el Comité de Calidad.

7.10.3 Personas que intervienen en las auditorías

Además de la Dirección de la empresa, que dirige directamente la Auditoría de la Política y de los Objetivos de la Calidad, las personas que intervienen, más frecuentemente, en las auditorías de la calidad son:

- Del propio departamento auditado:

  Cuando son los mandos los que realizan las auditorías de la calidad, la mayoría de las actividades analizadas son conocidas por ellos. En consecuencia, pueden enterarse de muchas cosas a través de la observación.

  La principal ventaja de utilizar personas del propio departamento es que los mandos creen más en sus propias observaciones que en las obtenidas por inspectores o auditores.

  Por el contrario, los principales inconvenientes radican en que los mandos no suelen disponer del tiempo no tener las condiciones necesarias para ser auditores. Normalmente no estudian a fondo los datos, la documentación y todos aquellos aspectos que no son los obtenidos por observación directa.

- Inspectores de la Calidad:

  En algunas empresas las personas de inspección suelen tener una independencia jerárquica respecto al objeto a auditar.

  En tales casos es económico utilizar a esos inspectores para realizar las auditorías de la calidad.

  Un inconveniente en la utilización de los inspectores propios es que no suelen tener el nivel jerárquico suficiente como para que las conclusiones de sus auditorías llamen la atención de la Dirección.

- Mandos de la empresa como auditores ocasionales:

  Cuando por situaciones de riesgo evidente o problemas puntuales, se necesita una gran experiencia en el tema a tratar, las empresas pueden utilizar mandos para auditar departamentos ajenos a su función.

  Una ventaja es que los mandos que realizan estas auditorías acaban teniendo una visión más clara del conjunto de la empresa.

  Un inconveniente es que si deben hacer compatibles sus tareas habituales con las auditorías que se les han encomendado, estas

auditorías suelen padecer esta situación.

El inconveniente puede ser solucionado liberando totalmente al mando de sus funciones habituales durante la realización de la auditoría.

- Personas de la empresa con dedicación ocasional, o total, a la realización de la auditoría:

  Normalmente, los auditores suelen depender jerárquicamente de Garantía o Ingeniería de Calidad. En estos casos es frecuente que a estos auditores se les encomiende los métodos y procesos de calidad. Es decir, su dedicación a las auditorías no es total.

  En estos casos, existe el riesgo que la presión de las tareas diarias sea tal, que se resiente la calidad de la auditoría o, que se retrase con el tiempo.

  Por el contrario, cuando la auditoría es realizada por personas cuya única misión en la empresa es la de hacer auditorías, los problemas mencionados dejan de existir. Además, estos auditores con dedicación total, suelen convertirse en unos profesionales cuyas observaciones gozan de gran credibilidad.

- Consultores externos:

  Deben ser profesionales altamente capacitados. Es aconsejable utilizar consultores externos para:

  - Efectuar la primera auditoría y crear la base para posteriores.
  - Cuando la Dirección de la empresa piensa que los miembros de su organización no son objetivos.
  - Agilizar, en los casos que los problemas de calidad llevan mucho tiempo sin ser resueltos.
  - Formar a los auditores internos.

7.11 FASES DE UNA AUDITORÍA DE CALIDAD

1) Establecer los objetivos de la Auditoría de Calidad. En la planificación de calidad de la organización hay que incluir las auditorías de calidad como instrumento de gestión. Con su empleo se deben perseguir especificaciones establecidas y poder aplicar las medidas apropiadas. Antes de comenzar a realizar una determinada auditoría hay que establecer qué desea lograrse con ella. Los objetivos concretos perseguidos ayudaran a establecer el tipo de auditoría más adecuado, además de su campo y profundidad.

2) Establecer el tipo de Auditoría según actividad y responsabilidad. Consiste en definir el objeto de la auditoría, así como decidir si va a ser interna o externa.

3) Establecer la frecuencia. Dado que el objetivo de las auditorías de calidad es la mejora continua, no tendría sentido no realizarlas de modo regular. Pero la frecuencia con que deben hacerse depende del objeto de la auditoría.

4) Designar a los auditores. El número y cualificación de los auditores depende del tipo y frecuencia con que se vayan a llevar a cabo. Si se precisa de un equipo auditor, es preciso nombrar a un jefe del equipo, que tendrá la responsabilidad del mismo.

5) Cualificación de los auditores. Dependiendo del tipo de auditoría hará falta conseguir una especial cualificación para las personas que vayan a llevar a cabo las auditorías. Sobre la formación específica de los auditores se habla con más detalle en el punto 7.9 "Perfil del auditor informático**".**

6) Preparar el Plan de Auditoría. El Plan de la Auditoría se emplea como base para proceder de una forma estructurada; en él se especifican todos los aspectos organizativos de las auditorías, como por ejemplo las entidades afectadas, orden del procedimiento, distribución de tareas, fechas, definición de responsabilidades.

7) Recoger información sobre las entidades objeto de la auditoría. Esta recogida de información es más importante cuando se trata de auditorías externas, ya que con ello se logra que el equipo auditor tome contacto con la filosofía y metas del a empresa, sus productos y procesos, la organización de la empresa, las tareas concretas y funcionamiento del área objeto de la auditoría, y las relaciones con clientes externos e internos.

8) Documentación. Se desarrolla en función del tipo de auditoría de que se trate. Hay que comprobar que los documentos necesarios están disponibles.

9) Preparar *checklist*, o lista de chequeo. Antes de hacer la auditoría hay que elaborar las *checklist* (listado con todos los aspectos que se van a revisar en la auditoría) que se van a emplear en la auditoría. En algunos casos no será necesario preparar dichas *checklist* porque ya estarán disponibles de auditorías previas. Las entidades de certificación y otras organizaciones publican *checklist* que pueden emplearse como base y modelos por las empresas.

10) Anunciar la auditoría y llevar a cabo las conversaciones iniciales. La unidad que va ser objeto de la auditoría tiene que ser informada con suficiente antelación. No se trata de un control por sorpresa. Hay que procurar que tengan el suficiente tiempo para prepararse para la auditoría. Además es importante que conozcan los objetivos de la auditoría y sean informados sobre todos los detalles importantes. Con ello conseguiremos lograr su colaboración, además garantizar la objetividad de la auditoría. En la reunión inicial se reúnen los miembros del equipo de auditoría con los máximos responsables de la entidad objeto de la auditoría y se les explica el plan que va a seguir la auditoría.

11) Llevar a cabo la Auditoría preliminar. Es una auditoría "de prueba" que se desarrolla un poco antes de la "verdadera" auditoría que ayuda a su preparación. Esta primera auditoría se identifican ya algunos problemas que pueden ser corregidos antes de que la auditoría se lleve a cabo.

Debe valorarse en cada caso si es necesario llevar a cabo esta fase.

12) Auditoría. En la realización de la auditoría de calidad se pretende estudiar si se cumplen las correspondientes especificaciones.

13) Informe de auditoría. En el informe de auditoría se presentan los resultados de la auditoría. Se expresan como una comparación entre lo que "debe ser" y lo "que es" en la realidad. Su profundidad y contenido depende del tipo de auditoría de que se trate, pero en lo esencial suele contener los siguientes puntos:

    - Informaciones generales, como fecha, departamento, tipo de auditoría.
    - Componentes del equipo auditor.
    - Objetivos de la auditoría.
    - Resultados de la comprobación.
    - Aspectos relevantes a considerar en el transcurso de una auditoría.

    No deben incluir comentarios ni propuestas de acciones de mejora; este punto corresponde a los responsables competentes.

14) Comprobar la eficacia del proceso de la auditoría. El propio proceso de la auditoría debería ser objeto de mejora continua; deben ser analizados los problemas y fallos que han surgido durante la auditoría, las propuestas que puedan venir tanto de los miembros del equipo de auditoría como del cuerpo auditado, para buscar potenciales de mejora. Además se debe estar pendiente a posibles cambios en las leyes, normas o recomendaciones.

    Es importante advertir que no todas las fases se presentan cada vez que se lleva a cabo una auditoría. Dependerá en gran medida de la complejidad, amplitud de la misma y si es la primera vez que se realiza o ya se ha realizado en otras ocasiones.

7.12 AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan.

El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otros ordenadores, no exista la posibilidad de transmisión de virus.

7.12.1 Políticas de seguridad informática

7.12.1.1 Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

7.12.1.2 Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

7.12.1.3 Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

7.12.1.4 Parámetros para Establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

7.12.1.5 Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercado por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

7.12.2 Privacidad en la red y control de intrusos (priv)

7.12.2.1 Privacidad en la Red

7.12.2.1.1 Generalidades

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Por tal razón, es necesario que las organizaciones m*antengan sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos*.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos

hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

7.12.2.1.2 Definición de Privacidad de las Redes

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.).

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos, ordenadores personales, teléfonos móviles, etc.).

7.12.2.1.3 Requisitos para Mantener la Privacidad de las Redes

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más seguras ante las posibilidades de intrusión.

1. **Disponibilidad**: significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la empresa.
2. **Autenticación**: confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, la autenticación de los sitios web, etc.
3. **Integridad**: confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica
4. **Confidencialidad**: protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos

almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

7.12.2.1.4 Riesgos o Amenazas a la Privacidad de las Redes

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

1. **Interceptación de las Comunicaciones**: la comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, pinchando la línea, o controlando las transmisiones.
2. **Acceso no Autorizado a Ordenadores y Redes de Ordenadores**: el acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma mal intencionado para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques aprovechando la tendencia de la gente a utilizar contraseñas previsibles, aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiable e interceptación de contraseñas.
3. **Perturbación de las Redes**: actualmente las redes se encuentran ampliamente digitalizadas y controladas por ordenadores, pero en el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos se concretan a los puntos débiles y más vulnerables de los componentes de las redes como son sistemas operativos, encaminadores, conmutadores, servidores de nombres de dominio, etc.
4. **Ejecución de Programas que Modifican y Destruyen los Datos**: los ordenadores funcionan con programas informáticos, pero lamentablemente, los programas pueden usarse también para desactivar un ordenador y para borrar o modificar los datos. Cuando esto ocurre en un ordenador que forma parte de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Por ejemplo, un virus es un programa informático mal intencionado que reproduce su propio código que se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.
5. **Declaración Falsa**: a la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. Para la red, el mayor riesgo de ataque procede de la gente que conoce el contexto. Por tal razón, las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos, como pueden ser transmitir datos confidenciales a personas no autorizadas, rechazo de un contrato, etc.
6. **Accidentes no Provocados**: numerosos problemas de seguridad se deben a accidentes imprevistos o no provocados como: son tormentas, inundaciones, incendios, terremotos, interrupción del servicio por obras de construcción, defectos de programas y

errores humanos o deficiencias de la gestión del operador, el proveedor de servicio o el usuario.

7.12.2.2 Detección de intrusos

7.12.2.2.1 Generalidades

Los sistemas computarizados y aplicaciones están en permanente evolución, por tal razón pueden surgir nuevos puntos vulnerables. A pesar de los avances en los sistemas de seguridad, los usuarios no autorizados con herramientas muy sofisticadas tienen grandes posibilidades de acceder a las redes, sistemas o sitios de las organizaciones e interrumpir sus operaciones.

Actualmente, existen más de 30.000 sitios en internet orientados a la piratería o intrusión de redes, los cuales ofrecen programas de fácil descarga y acceso que han dejados las puertas abiertas para nuevos ataques.

Entre los primeros intrusos o piratas informáticos famosos están Steve Wozniak, Bill Gates y Linus Torvalds, quienes ahora son reconocidos creadores de muchas de las tecnologías informáticas que utilizamos en la actualidad. Estos primeros intrusos de redes amaban la tecnología, sentían la imperiosa necesidad de saber cómo funcionaba todo y su objetivo era impulsar los programas que trascendieran el objetivo para el cual fueron diseñados. En ese entonces, la palabra intruso o pirata informático no tenía la connotación negativa que tiene hoy, ya que ha desaparecido la ética original que provenía de la simple curiosidad y la necesidad de afrontar desafíos.

Los objetivos de los primeros intrusos informáticos no podrían estar más ajenos a los objetivos de los piratas actuales. Lo que motiva a esta nueva generación no parece ser la curiosidad o el afán del conocimiento, como solía ser, al contrario, los motiva la codicia, el poder, la venganza y otras intenciones maliciosas.

7.12.2.2.2 Factores que Propician el Acceso de Intrusos a la Redes y Sistemas

Los ataques a la seguridad han sobrepasando las estimaciones esperadas, y además del crecimiento de los sitios de Internet relacionados con piratería, también hay otros aspectos que propician esta situación:

- Los sistemas operativos y las aplicaciones nunca estarán protegidos. Incluso si se protege el sistema nuevas vulnerabilidades aparecerán en el entorno todos los días, como las que actualmente representan los teléfonos, equipos inalámbricos y dispositivos de red.
- En las empresas las redes internas son más o menos confiables, ya que los empleados se conectan a la red desde la casa, otras oficinas u hoteles fuera de la empresa, lo cual genera nuevos riesgos.
- Falta de seguridad física en algunas empresas y falta de políticas de seguridad informática. Por ejemplo, muchos empleados se ausentan y dejan desprotegido su ordenador.

- Los empleados no siempre siguen y reconocen la importancia de las políticas de seguridad: La capacitación y entrenamiento que se les brinde a los empleados no cuenta mucho si ignoran las advertencias sobre los peligros de abrir los archivos adjuntos sospechosos del correo electrónico.
- Requerimientos cada vez mayores de disponibilidad de redes y acceso a ellas.

7.12.2.2.3 Medidas para Controlar el Acceso de Intrusos

Algunas medidas que se pueden poner en práctica para controlar los accesos de intrusos pueden ser las siguientes:

- Utilizar un firewall, que no es más que un dispositivo localizado entre el ordenador anfitrión y una red, con el objeto de bloquear el tráfico no deseado de la red mientras permite el cruce de otro tráfico.
- Utilización y actualización de antivirus.
- Actualizar todos los sistemas, servidores y aplicaciones, ya que los intrusos por lo general a través de agujeros conocidos de seguridad.
- Desactivar los servicios innecesarios de redes.
- Eliminar todos los programas innecesarios.
- Analizar la red en busca de servicios comunes de acceso furtivo y utilizar sistemas de detección de intrusos los cuales permiten detectar ataques que pasan inadvertidos a un firewall y avisar antes o justo después de que se produzcan, y
- Finalmente, establecer la práctica de crear respaldos o Backus.

Hay muchos dispositivos de seguridad que pueden utilizar las empresas para contrarrestar las amenazas a las que están expuestas, por eso, con frecuencia muchas terminan utilizando soluciones como los firewalls, sistemas de detección de intrusos, redes virtuales, etc. para obtener la protección total que necesitan en materia de seguridad. Debido al incremento de las amenazas y la naturaleza dinámica de los ataques, es necesario adoptar prácticas eficientes e implementar políticas de seguridad que nos permitan manejar eficientemente este tipo de ataques.

7.12.2.2.4 Principales Actividades de los Intrusos o Piratas Informáticos

Los comportamientos de los intrusos o piratas informáticos han tomado matices preocupantes. A continuación enumeramos algunas de estas actividades:

- Desfiguramiento de los sitios web: esto ocurre cuando se entra al servidor web y se altera o reemplaza la página principal. Los desfiguramientos de los sitios web es una práctica común, pues se lleva a cabo simplemente descargando de Internet un programa que está diseñado para aprovecharse de las vulnerabilidades de los sistemas.
- Hurto de la información de las tarjetas de crédito: La información de la tarjeta de crédito puede ser hurtada por medio de las

mismas herramientas de ataque que están tras los desfiguramientos de los sitios web. Una vez los piratas informáticos tienen acceso a la red, pueden analizar las bases de datos en busca de archivos que puedan tener información valiosa, como archivos de clientes. Todo archivo que sea interesante para el intruso puede ser descargado a su ordenador.

- Ataque a los programas instructores del servidor: Los programas instructores del servidor permiten las comunicaciones bidireccionales entre los servidores y usuarios web. Las instrucciones del servidor también es un objetivo común de los intrusos y lo hacen ejecutando comandos, leyendo los archivos del sistema o modificando los mismos.
- Ataques de negación de servicio: la negación de servicio se produce cuando alguien o algo impide que se realice una tarea u operación deseada. Los intrusos o piratas logran esto principalmente con el consumo del ancho de banda, inundando la red con datos, agotando los recursos del sistema, fallas de programación, etc.
- Ataques de negación distribuida de servicio: se refiere cuando muchos ordenadores se asaltan y se les ordena inundar un sitio determinado con paquetes o solicitud de información, negando así el servicio a usuarios legítimos.

7.12.3 Virus y antivirus (V/A)

7.12.3.1 Virus

7.12.3.1.1 Generalidades

Antes de profundizar en este tema, debemos aclarar que los virus de ordenadores son simplemente programas, y como tales hechos por programadores. Son programas que debido a sus características particulares son especiales. Para hacer un virus de ordenador no se requiere capacitación especial, ni una genialidad significativa, sino conocimientos de lenguajes de programación para el público en general y algunos conocimientos puntuales sobre el ambiente de programación y arquitectura de los PC's.

Nuestro trabajo capta el problema del virus, desde el punto de vista funcional. En la vida diaria, cuando un programa invade inadvertidamente el sistema, se replica sin conocimiento del usuario y produce daños, pérdida de información o fallas del sistema, reconocemos que existe un virus. Los virus actúan enmarcados por "debajo" del sistema operativo, como regla general, y para actuar sobre los periféricos del sistema, tales como disco rígido, disqueteras, ZIP's CD-R's, hacen uso de sus propias rutinas aunque no exclusivamente. Un programa normal, por llamarlo así, utiliza las rutinas del sistema operativo para acceder al control de los periféricos del sistema, y eso hace que el usuario sepa exactamente las operaciones que realiza, teniendo control sobre ellas. Los virus, por el contrario, para ocultarse a los ojos del usuario, tienen sus propias rutinas para conectarse con los periféricos del ordenador, lo que les garantiza cierto grado de inmunidad a los ojos del

usuario, que no advierte su presencia, ya que el sistema operativo no refleja su actividad en el PC. Una de las principales bases del poder destructivo de estos programas radica en el uso de funciones de manera "sigilosa", oculta a los ojos del usuario común.

El virus, por tratarse de un programa, para su activación debe ser ejecutado y funcionar dentro del sistema al menos una vez. Demás está decir, que los virus no surgen de los ordenadores espontáneamente, sino que ingresan al sistema inadvertidamente para el usuario, y al ser ejecutados, se activan y actúan con el ordenador huésped.

7.12.3.1.2 Definiciones

1. "Un virus es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco."
2. Un virus es una porción de código ejecutable, que tiene la habilidad única de reproducirse. Se adhieren a cualquier tipo de archivo y se diseminan con los archivos que se copian y envían de persona a persona.

Además de reproducirse, algunos virus informáticos tienen algo en común: una rutina dañina, que el virus descarga como una bomba, mientras que las descargas pueden ser simples mensajes o imágenes, estas también pueden borrar archivos, reformatear el disco duro o causar otro tipo de daño. Si el virus no contiene una rutina dañina, aún puede causar problemas, como tomar espacio libre del disco y de la memoria, y también disminuir el rendimiento del ordenador.

Los virus de los ordenadores no son más que programas; y estos virus casi siempre los acarrean las copias ilegales o piratas. Provocan desde la pérdida de datos o archivos en los medios de almacenamiento de información (disquete, disco duro, cinta), hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo.

7.12.3.1.3 Características

Hay que recordar que un virus no puede ejecutarse por sí solo, pues necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse en un programa portador, el virus precisa modificar la estructura de aquél, posibilitando que durante su ejecución pueda realizar una llamada al código del virus.

Las particularidades de los virus:

- Son muy pequeños.
- Casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha de creación.
- Se reproducen a sí mismo.
- Toman el control o modifican otros programas.
- **Es dañino**: El daño es implícito, busca destruir o alterar, como el consumo de memoria principal y tiempo de procesador.

- **Es autorreproductor**: A nuestro parecer la característica más importante de este tipo de programas es la de crear copias de sí mismo.
- **Es subrepticio:** Esto significa que utilizará varias técnicas para evitar que el usuario se dé cuenta de su presencia.

7.12.3.1.4 ¿Quiénes hacen los virus?

Los virus informáticos son hechos por personas con conocimiento de programación, pero que no son necesariamente genios de los ordenadores. Tienen conocimiento de lenguaje ensamblador y de cómo funciona internamente el ordenador. A diferencia de los virus que causan resfriados y enfermedades en humanos, los virus computacionales no ocurren de forma natural, cada uno es programado. No existen virus benéficos. Algunas veces son escritos como una broma, desplegando un mensaje humorístico. En estos casos, el virus no es más que una molestia. Muchas veces son creados por personas que se sienten aburridas, con coraje, como reto intelectual; cualquiera que sea el motivo, los efectos pueden ser devastadores.

7.12.3.1.5 Síntomas más comunes de virus

La mejor forma de detectar un virus es, obviamente un antivirus, pero en ocasiones los antivirus pueden fallar en la detección. Puede ser que el escaneo no detecte nada y sí el análisis heurístico. Puede ser que no detectemos nada y aún seguir con problemas. En estos casos debemos notar algunos síntomas posibles:

- Los programas comienzan a ocupar más espacio de lo habitual. Se reduce el espacio libre en la memoria RAM. El virus al entrar en el sistema, se sitúa en la memoria RAM, ocupando una porción de ella. El tamaño útil y operativo de la memoria se reduce en la misma cuantía que tiene el código del virus. Siempre en el análisis de una posible infección es muy valioso contar con parámetros de comparación antes y después de la posible infección. Por razones prácticas casi nadie analiza detalladamente su PC en condiciones normales y por ello casi nunca se cuentan con patrones antes de una infección, pero sí es posible analizar estos patrones al arrancar un PC en la posible infección y analizar la memoria arrancando el sistema desde un disco libre de infección.
- Aparecen o desaparecen archivos. En mayor o menor medida, todos los virus, al igual que programas residentes comunes, tienen una tendencia a "colisionar" con otras aplicaciones, lo que provoca también aparición de mensajes de error no comunes.
- Cambia el tamaño de un programa o un objeto. Programas que normalmente funcionaban bien, comienzan a fallar y generar errores durante la sesión.
- Aparecen mensajes u objetos extraños en la pantalla. El código viral, ocupa parte de la RAM y debe quedar "colgado" de la memoria para activarse cuando sea necesario. Esa porción de código que queda en RAM, se llama residente y con algún utilitario que analice el RAM puede ser descubierto.

- El disco trabaja más de lo necesario. Tiempos de cargas mayores y es debido al enlentecimiento global del sistema, en el cual todas las operaciones se demoran más de lo habitual.
- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados. Las operaciones se realizan con más lentitud, ya que los virus son programas y como tales requieren de recursos del sistema para funcionar y su ejecución al ser repetitiva, lleva a un enlentecimiento y distorsión global en las operaciones.
- Se modifican sin razón aparente el nombre de los ficheros.
- No se puede acceder al disco duro.

7.12.3.1.6 Clasificación

A continuación esbozamos una clasificación que tiende a catalogar los virus actuales, sin intentar crear una clasificación académica, sino una orientación en cuanto a funcionalidad de los virus:

- **Virus de Macros/Código Fuente:** Se adjuntan a los programas fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hojas de Cálculo (Excel, Quattro, Lotus).
- **Virus Mutantes:** Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (NATAS o SATÁN, Miguel Ángel, por mencionar algunos).
- **Gusanos:** Son programas que se reproducen a sí mismo y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posesionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdidas de datos.
- **Caballos de Troya:** Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
- **Bomba de Tiempo:** Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y sólo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.
- **Autorreplicables:** Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se autoreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programada o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo

de estos es el virus del viernes 13, que se ejecuta en esa fecha o se borra (junto con los programas infectados), evitando así ser detectado.

- **Infectores del área de carga inicial:** Infectan los disquetes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende el ordenador y lo conservan todo el tiempo.
- **Infectores del sistema:** Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).
- **Infectores de programas ejecutables:** Estos son los virus más peligrosos porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras). La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posesiona en la memoria del ordenador y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos.

Todos estos programas tienen en común la creación de efectos perniciosos, sin embargo, no todos pueden ser considerados como virus propiamente dichos. La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas.

7.12.3.1.7 Ciclo de Infección

Como mencionamos con anterioridad, para que un virus se active en memoria, se debe ejecutar el programa infectado en primer término, para que el virus inicie sus actividades dentro de nuestro sistema. En este caso, no es necesario arrancar ningún programa, sino simplemente abrir un archivo de Word o Excel infectado.

El ciclo completo de infección de un Macro Virus sería así:

- Se abre el archivo infectado, con lo cual se activa en memoria.
- Infecta sin que el usuario se dé cuenta al NORMAL.DOT, con eso se asegura que el usuario sea un reproductor del virus sin sospecharlo.
- Si está programado para eso, busca dentro del PC los archivos de Word, Excel, etc. que puedan ser infectados y los infecta.
- Si está programado, verifica un evento de activación, que puede ser una fecha, y genera el problema dentro del PC (borrar archivos, destruir información, etc.).
- Ahora bien, en el caso de mails vía Internet. Los mails no son programas. Algunos no poseen macros (los que sí poseen

macros son los mails de Microsoft Outlook). Aquellos que no tienen lenguaje de macros (NO PUEDEN CONTENER VIRUS).

- Los archivos adjuntos asociados al mail pueden llevar virus (siempre que sean susceptibles de ser infectados). Bajen el adjunto, y verifíquenlo. Asegúrense que el antivirus chequee los zipeados o comprimidos si lo adjuntado es un archivo de ese tipo. Si el adjunto es un documento que puede tener macros, desactiven las macros del programa Word antes de abrirlo. Si el adjunto es un archivo de texto plano, pueden quedarse tranquilos.

7.12.3.1.8 Medidas de Protección Efectivas

Obviamente, la mejor y más efectiva medida es adquirir un antivirus, mantenerlo actualizado y tratar de mantenerse informado sobre las nuevas técnicas de protección y programación de virus. Gracias a Internet es posible mantenerse al tanto a través de servicios gratuitos y pagos de información y seguridad. Hay innumerables boletines electrónicos de alerta y seguridad que advierten sobre posibles infecciones de mejor o menor calidad. Existen herramientas indispensables para aquellos que tienen conexiones prolongadas a Internet, que tienden a proteger al usuario no sólo detectando posibles intrusos dentro del sistema, sino chequeando constantemente el sistema, a modo de verdaderos escudos de protección.

7.12.3.2 Antivirus

7.12.3.2.1 Generalidades

El programa de antivirus debe ser completo, preciso y rápido. Si no es así, usted simplemente no lo utilizará, y dejará a un lado esta actividad, lo cual es muy peligroso. Por ejemplo, en cualquier mes determinado hay de 200 a 300 virus circulando por el mundo. Esa cifra proviene de la WildList, una lista mensual reconocida internacionalmente, que tiene los virus que se dispersan en el mundo "en estado salvaje".

El método principal de un analizador de antivirus para atrapar los virus es comparar un código sospechoso con las bases de datos de conocidas firmas de virus. Estas bases de datos incluyen nombres actuales o anteriores en la WildList, así como decenas de miles "zoo virus", que en su mayoría existen en laboratorios, pero que utilizan trucos que pueden ser empleados por futuros virus.

Con el propósito de adquirir un buen antivirus, lo primero es verificar el tipo de tecnología aplicada en su desarrollo, actualmente los antivirus utilizan dos técnicas de verificación:

- La conocida técnica de escaneo, consistente en tener una gran base de datos con fragmentos víricos para comparar los archivos con esa inmensa biblioteca del wildlist.
- La tecnología heurística es fundamental en estos momentos, y en mi opinión, los antivirus han de ofrecer como alternativa al escaneo común (aún necesario) la búsqueda heurística. Esta técnica permite detectar virus que aún no estén en la base de datos scaning, y es muy útil cuando padecemos la infección de

un virus que aún no ha sido estudiado ni incorporado a los programas antivirus.

7.12.3.2.2 Definición de Antivirus

- Es el programa que se encarga de analizar el contenido de los ficheros y, en caso de detectar un virus en su interior, proceder a su desinfección. También realizan búsquedas heurísticas, esto es, buscar funciones que puedan resultar nocivas para tu ordenador, sin que sean virus reconocidos.
- Es una aplicación o programa dedicada a detectar y eliminar virus informáticos. La forma en que protege es la siguiente, el sistema de protección del Antivirus depende del sistema operativo en que se esté trabajando. Por término general se puede pensar en un programa que vigila todos y cada uno de los accesos que se realizan a ficheros y discos y antes de autorizarlos avisa de la existencia virus y, en su caso, desinfecta el fichero en cuestión.

Si eres muy cuidadoso con los programas que utilizas, la información que introduces a tu ordenador y con los lugares que visitas en el Internet, así como intercambiar tus discos en el trabajo o discos de amigos (duda procedencia) es muy posible que nunca tengas problemas con virus, lo que sí, es indispensable que tengas instalado un buen Antivirus.

7.12.3.2.3 Los Antivirus Más Buscados

Actualmente, los virus no sólo son más potentes que sus predecesores, sino que se propagan más rápido. En los años 80, los virus del sector de arranque se multiplicaban a través del intercambio de discos flexibles. A finales de los 90, el correo electrónico era quien transportaba virus de macros que venían en documentos anexos de Microsoft Word.

Ahora el peligro viene principalmente de los gusanos de envíos masivos, se auto replican y son capaces de secuestrar los libros de direcciones de correo electrónico y auto enviarse a múltiples destinatarios. Por ejemplo, LoveLetter era un virus de guión en Visual Basic. Hoy, la mayoría de los gusanos de correo masivo son programas Win32 independientes, como en el caso de SirCam y Klez. Estos programas son lo peor de todas las infecciones de virus.

Por su parte, los virus de los macros están en un distante segundo lugar y los de guión vienen pegados en un tercer lugar. Ahora los virus del sector arranque sólo representan cerca del 1% de las infecciones.

Al elegir un antivirus, tomamos en cuenta tres aspectos fundamentales: facilidad de adquisición de las actualizaciones, menor costo posible y facilidad de uso.

7.12.3.2.4 Antivirus al Rescate

Además de la clase de virus que el analizador descubre, también es importante la ubicación de éste, por ejemplo, el protector antivirus debe ser capaz de meterse bien dentro de los archivos zip y otros archivos comprimidos, incluso hasta en los archivos zip que estén ubicados dentro de otros archivos zip. También debe revisar los anexos al correo

electrónico, y donde quiera que descubra una infección, debe eliminarla sin destruir archivos valiosos.

Kaspersky, McAfee, Norton, Panda y PC-cillin interceptan y analizan los anexos al correo electrónico antes de que lleguen a la unidad de disco duro. Pero Norton y PC-cillin sólo funcionan con programas de correo electrónico que cumplan con los requisitos de POP3, mientras que Kaspersky sólo funciona con los clientes de Outlook, Outlook Express y Exchange, de Microsoft, Panda, a su vez, analiza anexos de POP3, Exchange e incluso de AOL.

7.12.3.2.5 Conozca Bien su Antivirus

Debido a que en todo momento aparecen nuevos virus, es necesario actualizar con facilidad las definiciones. Todos los programas probados, excepto Etrust, ofrecen actualizaciones automáticas programadas. Sin embargo, nuestro tanto a favor es para Norton, que revisa si hay actualizaciones de manera prefijada, al momento de ser instalado y después, cada 4 horas. Norton también gana puntos por tener la interfaz más lógica, de fácil dominio.

En virtud de lo anterior, al hacer una evaluación es importante tratar de verificar hasta qué punto los diversos antivirus cumplen con las siguientes características:

1. Deben actualizar los patrones o firmas, por lo menos una vez por semana.
2. La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.
3. Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.
4. Se deben poder adaptar a las necesidades de diferentes usuarios.
5. Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
6. Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.
7. Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.
8. Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.
9. No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.

10. El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible.
11. Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.
12. Deben de tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

En base a estos parámetros, uno mismo puede poner a prueba los distintos productos que hay en el mercado y de acuerdo a nuestras prioridades sacar conclusiones.

7.12.3.2.6 Importancia del Antivirus

Actualmente, no es difícil suponer que cada vez hay más personas que están conscientes de la necesidad de hacer uso de algún antivirus como medida de protección básica.

- Desde el punto de vista del administrador, este desea primordialmente tener resultados al problema de administración centralizada. Es decir, desea que un antivirus posea una consola que permita la instalación remota tanto en una red LAN como en una WAN y no verse obligado a instalar el producto a pie en cada una de las estaciones de trabajo.
- Desde el punto de vista del usuario final, a quien le interesa no infectarse por ningún motivo y que la protección en memoria del producto sea de lo más eficaz, tanto para detectar y remover cualquier virus que pueda presentarse.

Basados en estas necesidades, podemos darles los siguientes puntos:

f.1. Controles

- Control de acceso físico a los equipos.
- Control de entradas a los programas del ordenador a través de claves de acceso (passwords).
- Registro, verificación y control de los disquetes, cd's que se introducen al ordenador.
- Se recomienda algún programa de tipo menú que restrinja los programas que se pueden ejecutar a sólo los autorizados a cada usuario.

f.2. Bloqueos

- Cerradura para floppies "drive lock"
- Uso del candado o llave de encendido, si el ordenador lo tiene.
- Deshabilitar el arranque desde la unidad de disquete.
- Deshabilitar completamente las unidades de disquete.
- Habilitación de la facilidad de palabra clave (password).
- Activar la protección antivirus en BIOS.

f.3. Disquetes

Estos son puntos muy importantes, ¡prácticamente todos los virus se introducen a un ordenador por medio de disquetes! Y en caso de un desastre, las copias de respaldo en disquete serán la salvación de nuestros datos.

- Verificar contra virus todos los disquetes que se introduzcan en el ordenador, aunque sólo sean de datos.
- No ejecutar programas de origen dudoso.
- No meter disquetes extraños.
- Nunca arranque desde disquete en la operación normal de su ordenador.
- Nunca dejar puestos disquetes al apagar el ordenador.
- Tenga un disquete de arranque que esté libre de virus y protegido contra escritura.
- Si es necesario arrancar desde disquete, utilice únicamente este disquete.
- Proteja contra escritura sus discos del sistema, así como sus discos de programas de aplicación.
- Que los usuarios sólo manejen disquetes de datos y nunca de programas.
- Instalar nuevos paquetes en una máquina que sirva de conejillo de Indias y que esté un tiempo en observación.
- Mantener copias respaldo, tanto de los programas, como de los datos.
- Hacer por separado los respaldos de datos y de programas.

f.4. Vacunas Antivirus

- Tener varios programas antivirus, preferentemente con diferentes enfoques.
- Utilizar o activar las diversas opciones de protección.
- Comprar las versiones actualizadas de las vacunas.
- Leer la documentación y manuales de los antivirus.

f.5. Servicios en Línea

- Verificar contra virus todo programa que se transfiera.
- Verificar contra virus todo archivo autodescomprimible (aunque sea de datos).

f.6. Otros

- Capacitar a los usuarios en protección contra virus.

- Desarrollar un plan de emergencia contra virus que prevea procedimientos o máquinas alternas para el proceso de los datos.
- Mantenerse informado, o sea leer sobre el tema.

7.12.4 Seguridad

7.12.4.1 Generalidades

Cuando hablamos de realizar una evaluación de la seguridad es importante conocer cómo desarrollar y ejecutar la implantación de un sistema de seguridad.

Desarrollar un sistema de seguridad significa *"planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa"*.

Las consideraciones de un sistema integral de seguridad deben contemplar:

- Definir elementos administrativos.
- Definir políticas de seguridad.
  - A nivel departamental.
  - A nivel institucional.
- Organizar y dividir las responsabilidades.
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.).
- Definir prácticas de seguridad para el personal.
- Plan de emergencia, plan de evacuación, uso de recursos de emergencia como extinguidores.
- Definir el tipo de pólizas de seguros.
- Definir elementos técnicos de procedimientos.
- Definir las necesidades de sistemas de seguridad para hardware y software.
- Flujo de energía.
- Cableados locales y externos.
- Aplicación de los sistemas de seguridad incluyendo datos y archivos.
- Planificación de los papeles de los auditores internos y externos.
- Planificación de programas de desastre y sus pruebas (simulación).
- Planificación de equipos de contingencia con carácter periódico.
- Control de desechos de los nodos importantes del sistema.
- Política de destrucción de basura, copias, fotocopias, etc.

Para dotar de medios necesarios al elaborar su sistema de seguridad se debe considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos y ambientales.
- Elaborar un plan para un programa de seguridad.

7.12.4.2 Seguridad del Correo

Cada día son más las organizaciones que utilizan el correo electrónico como herramienta fundamental de sus negocios, por ende, es indispensable que se cuente con soluciones confiables y escalables que permitan que las comunicaciones, utilizando este tipo de medio, se realicen de forma segura y confiable. La nueva versión del programa de administración de listas de correo electrónico LISTSERV, viene a satisfacer esta demanda, pues está repleta de nuevas y mejoradas características, está dotada de protección contra virus y de una mayor facilidad de uso.

LISTSERV trabaja bajo una interfaz rediseñada tipo Web que facilita la administración de la lista. Incluye un Experto de Tarea, que guía al administrador de la lista con instrucciones detalladas paso a paso.

Asimismo, con la proliferación de los virus a través del correo electrónico, L-Soft ha integrado a su lista el programa de protección contra virus de F-Secure para inspeccionar el correo electrónico.

7.12.4.3 ¿Cómo Puede Elaborar un Protocolo de Seguridad Antivirus?

La forma más segura, eficiente y efectiva de evitar virus, consiste en elaborar un protocolo de seguridad para sus sistemas PC's. Un protocolo de seguridad consiste en una serie de pasos que deberá seguir con el fin de crear un hábito al operar normalmente con programas y archivos en sus ordenadores. Un buen protocolo es aquel que le inculca buenos hábitos de conducta y le permite operar con seguridad su ordenador, aún cuando momentáneamente esté desactivado o desactualizado su antivirus.

Este protocolo establece ciertos requisitos para que pueda ser cumplido por el operador en primer término y efectivo en segundo lugar. Le aseguramos que un protocolo puede ser muy efectivo pero si es complicado, no será puesto en funcionamiento nunca por el operador.

El protocolo de seguridad antivirus consiste en:

1. Instalar el antivirus y asegurar cada 15 días su actualización.
2. Chequear los CD-Rom's ingresados en nuestro PC sólo una vez, al comprarlos o adquirirlos y marcarlos con un marcador para certificar el chequeo. Esto solo es válido en el caso de que nuestros CD's no sean procesados en otros ordenadores y sean regrabables.
3. Formatear todo disquete virgen que compremos, sin importar si son formateados de fábrica, ya que pueden colarse virus aún desde el proceso del fabricante.
4. Revisar todo disquete que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido ingresado en la disquetera de otro PC.

5. Si nos entregan un disquete y nos dicen que está revisado, no confiar nunca en los procedimientos de otras personas que no seamos nosotros mismos. Nunca sabemos si esa persona sabe operar correctamente su antivirus. Puede haber revisado sólo un tipo de virus y dejar otros sin controlar durante su escaneo, o puede tener un módulo residente que es menos efectivo que nuestro antivirus.
6. Para bajar páginas de Internet, archivos ejecutables, etc., definir siempre en nuestro PC una carpeta o directorio para recibir el material. De ese modo sabemos que todo lo que bajemos de Internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.
7. Nunca abrir un adjunto de un email sin antes chequearlo con nuestro antivirus. Si el adjunto es de un desconocido que no nos avisó previamente del envío del material, directamente borrarlo sin abrir.
8. Al actualizar el antivirus, verificar nuestro PC completamente. En caso de detectar un virus, proceder a verificar todos nuestros soportes (disquetes, CD's, ZIP's, etc.)
9. Si por nuestras actividades generamos grandes bibliotecas de disquetes conteniendo información, al guardar los disquetes en la biblioteca, verificarlos por última vez, protegerlos contra escritura y fecharlos para saber cuándo fue el último escaneo.
10. Haga el backup periódico de sus archivos. Una vez cada 15 días es lo mínimo recomendado para un usuario doméstico. Si usa con fines profesionales su PC, debe hacer backup parcial de archivos cada 48 horas como mínimo. Backup parcial de archivos es la copia en disquete de los documentos que graba.

7.12.4.4 Etapas para Implantar un Sistema de Seguridad

Para que su plan de seguridad entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguientes ocho pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.
5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

7.12.4.5 Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

7.12.4.6 Disposiciones que Acompañan la Seguridad

Desde el punto de vista de seguridad, se debe contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo, a saber:

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
- Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- Verificar el tipo de acceso que tiene las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación y viceversa.
- Que los operadores no sean los únicos en resolver los problemas que se presentan.

7.13 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

7.13.1 Cuestionarios

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otros medios la información que aquellos preimpresos hubieran proporcionado.

7.13.2 Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es sólo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

7.13.3 Checklist

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación.

Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

- Muy deficiente.
- Deficiente.
- Mejorable.
- Aceptable.
- Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente.

Basta con que el auditor lleve un pequeño guión. La cumplimentación de la Checklist no debe realizarse en presencia del auditado.

-¿Existe personal específico de vigilancia externa al edificio?

-No, solamente un guarda por la noche que atiende además otra instalación adyacente.

<Puntuación: 1>

-Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?

-Sí, pero sube a las otras 4 plantas cuando se le necesita.

<Puntuación: 2>

-¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

-Sí, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.

<Puntuación: 2>

-El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Ordenadores?

-No, solo tiene tarjeta el Jefe de Comunicaciones.

No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binaria:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

-¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

-¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

-¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

-¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

-¿Se conoce la norma anterior?

<Puntuación: 0>

-¿Se aplica en todos los casos?

<Puntuación: 0>

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <sí o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

7.13.4 Trazas y/o Huellas

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de Accounting o de contabilidad, en donde se encuentra la producción completa de aquél, y los Log* de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.

**Log:*

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

7.13.5 Software de Interrogación

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente paquetes de auditoría, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente -Servidor ", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre ordenadores personales y mainframe, de modo que el auditor informático copia en su propio PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Textos, paquetes de Gráficos, Hojas de Cálculo, etc.

7.14 METODOLOGIAS PARA LA APLICACIÓN DE LAS AUDITORÍAS DE LA CALIDAD

7.14.1 Desarrollo de las auditorías

Como ya sabemos, hay diferentes tipos de Auditorías de la Calidad, pero existen unas características comunes al desarrollo de todas ellas:

- Antes de comenzar una Auditoría de la Calidad, ésta debe estar autorizada por el Comité de Calidad.
- Dentro del Plan Anual de la Calidad, la Dirección debe haber desarrollado un Plan de Auditorías de la Calidad en el que se especifique:
  - La profundidad y la extensión de las auditorías.
  - Las misiones, las responsabilidades y el grado de independencia de los auditores.
  - La formación de los auditores (general y en las normas y procedimientos que van a ser auditados).
  - Los sistemas de presentación de los resultados.
  - La aprobación de los resultados
- Antes de auditar se debe tener preparado:
  - La norma con relación a la cual se audita.
  - El sistema de calificación elegido.
  - El sistema de puntuación en cada concepto.
  - El peso de cada apartado en relación con el total.
- Antes de auditar se debe haber informado al auditado de:
  - Qué es lo que se va a auditar.
  - Cuándo se va a auditar.
  - Cómo se va a auditar.
- Durante la actuación, el auditor debe tener:
  - Acceso a la documentación generada por la función de la Calidad.
  - Facilidad para el desempeño de la misión.
- Antes de la presentación del informe de la Dirección, es necesario:
  - Comentar los puntos débiles encontrados con las personas afectadas, con el fin de contrastar pareceres e identificar posibles errores del auditor.
  - En caso de discrepancias entre el auditor y la persona afectada, volver a tomar los datos, lo cual deberá ser reseñado en el informe.
  - Si un grupo de auditores está trabajando en una auditoría, mantener reuniones internas de coordinación tanto para intercambio de información como para priorizar los puntos débiles hallados y las recomendaciones a hacer a la Dirección.
- En la presentación de la Dirección el auditor informa, actúa como notario de un hecho constatado. No es responsabilidad del auditor la iniciación de un Plan de Mejora.

- De la Dirección emanarán:
  - Las conclusiones del informe.
  - Las pautas a seguir.
  - Las acciones de mejora.
  - Los plazos de ejecución.

Cuando se vuelve a auditar algo ya auditado anteriormente, es preciso tener en cuenta lo indicado en las acciones de mejora aprobadas por la Dirección, con objeto de que el auditor pueda informar de su progreso.

7.14.2 Métodos para la realización de auditorías

Esta metodología es utilizable cuando se pretende auditar todo el Sistema de la Calidad de la empresa, o una parte del mismo. Como base de referencia se suelen tomar las Normas Internaciones de Aseguramiento de la Calidad, adaptadas a las necesidades especificas.

Los pasos a dar son los siguientes:

- Dividir el Sistema de la Calidad en actividades a valorar.
- Asignar, a cada cuestión, un peso (P) que refleja la importancia relativa de la pregunta en el Sistema de la Calidad.
- Evaluar la respuesta a la cuestión, asignándole de 0 a 9 puntos, de acuerdo con la siguiente tabla:

V	NIVEL
0	Actividad/elemento **desconocido** en la entidad y/o no comprendido en su Sistema de Calidad.
1	Actividad/elemento **teóricamente conocido, no incluido** en el Sistema de la Calidad de la entidad, al cual no se presta atención en la mayor parte de los casos. **Responsabilidad no identificable.**
2	Actividad/elemento **conocido e incluido** en el Sistema de la Calidad de la empresa, al cual no se presta atención en la mayor parte de los casos. **Responsabilidad no aplicable.**
3	Actividad/elemento **comprendido** en el Sistema de la Calidad de la Entidad pero cuya **responsabilidad no está claramente identificada. Aplicación** práctica no sistemática, **confiada a la buena voluntad.**
4	Actividad/elemento incluido en el Sistema de la Calidad de la entidad cuya **responsabilidad** está **definida,** pero con **aplicación** práctica **no sistemática**. La **planificación** está **subordinada** a la decisión del responsable y **no** se encuentra **formalizada.**

5	Actividad/elemento incluido en el Sistema de la Calidad de la empresa pero con un **nivel de planificación inadecuado**. Su aplicación puede ser impuesta haciendo uso de la autoridad, lo cual afecta negativamente al operador, y comporta una elevada probabilidad de que la orden no sea seguida correctamente o ni siquiera escuchada.
6	Actividad/elemento incluido en el Sistema de la Calidad de la empresa, pero **aplicado** por el personal **con algunas desviaciones** respecto a lo establecido.
7	Actividad/elemento incluido en el Sistema de la Calidad de la entidad, generalmente **aplicado de forma correcta. Su aplicación es impuesta haciendo uso de la autoridad pero no se presta atención a su compresión** por parte del personal.
8	Actividad/elemento incluido en el Sistema de la Calidad de la entidad. **Planificación adecuada** y **ejecución sistemática** por parte del personal específico, que comprende el por qué del procedimiento establecido.
9	Actividad/elemento incluido en el Sistema de la Calidad de la entidad. En éste área, la empresa ha introducido innovaciones tales que hacen innecesarias las recomendaciones específicas.

Tabla 4: Métodos para realizar auditorías, tabla de respuestas

La puntuación máxima asignable a cada pregunta es 9 y, V la puntuación real otorgada. El grado de cumplimiento de cada cuestión, en tanto por ciento es:

$$(V/9) \times 100$$

Según el grado de cumplimiento de cada cuestión, el aspecto considerado presentara un riesgo de no-aseguramiento de la calidad, de acuerdo con la siguiente tabla:

Grado de Cumplimiento	Nivel de Riesgo
85 – 100	Ninguno
70 – 84.9	Limitado
61 – 69.9	Medio
51 - 60.9	Elevado
0 - 50.9	Cierto

Tabla 5: Grado de cumplimiento / Nivel de riesgo

- Determinar, para cada actividad del Sistema de la Calidad, su grado de cumplimiento, según:

$$\frac{\Sigma\ (V \times P)}{\Sigma\ (9 \times P)} \times 100$$

En donde el sumatorio incluye todas las cuestiones de la actividad valorada.

- Una relación exhaustiva de las cuestiones planteadas y las correspondientes respuestas a las mismas.
- Para cada actividad se señala su grado global de cumplimiento, así como los principales puntos débiles y puntos fuertes encontrados.
- Para la totalidad del Sistema de la Calidad se señala cuáles son las principales actividades débiles y fuertes.
- Para la totalidad del Sistema de la Calidad, se indican unas recomendaciones, en su orden de prioridad.

7.15. METODOLOGÍA DE TRABAJO DE AUDITORÍA

7.15.1 Estudio Inicial

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

Para su realización el auditor debe conocer lo siguiente:

7.15.1.1 Organización

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental.

Para realizar esto en auditor deberá fijarse en:

- *Organigrama:*

  El organigrama expresa la estructura oficial de la organización a auditar.

  Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

- *Departamentos:*

  Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección.

  El equipo auditor describirá brevemente las funciones de cada uno de ellos.

- *Relaciones Jerárquicas y funcionales entre órganos de la Organización:*

  El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

  Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

- *Flujos de Información:*

  Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.

  Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

  En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

  Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

- *Número de Puestos de trabajo*

  El equipo auditor comprobará que los nombres de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.

  Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

  Esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

- *Número de personas por Puesto de Trabajo*

  Es un parámetro que los auditores informáticos deben considerar.

  La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

7.15.1.2 Entorno Operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

- Situación geográfica de los Sistemas:

Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

- Arquitectura y configuración de Hardware y Software:

  Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías.

  Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

- Inventario de Hardware y Software:

  El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc.

  El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

- Comunicación y Redes de Comunicación:

  En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.

  Igualmente, poseerán información de las Redes Locales de la Empresa.

7.15.1.3 Aplicaciones Bases de Datos y Ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- Volumen, antigüedad y complejidad de las Aplicaciones
- Metodología del Diseño

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

- Documentación

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

La documentación de programas disminuye gravemente el mantenimiento de los mismos.

- Cantidad y complejidad de Bases de Datos y Ficheros.

El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

Estos datos proporcionan una visión aceptable de las características de la carga informática.

7.15.1.4 Determinación de recursos de la Auditoría Informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

7.15.1.4.1 Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.

Los recursos materiales del auditor son de dos tipos:

- Recursos materiales Software

  Programas propios de la auditoría: Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

  Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

- Recursos materiales Hardware

  Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en los Ordenadores del auditado.

  Para lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

7.15.1.4.2 Recursos Humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable.

Es igualmente reseñable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Perfiles Profesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

Tabla 6: Perfiles profesionales de los auditores informáticos

7.15.2 Actividades de la Auditoría Informática

Auditoría por temas generales o por áreas específicas:

La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de Trabajo:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.

- Muestreos.

Herramientas:

- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

7.15.3 Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del informe final:

El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

Definición de objetivos y alcance de la auditoría.

Enumeración de temas considerados:

Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

Cuerpo expositivo:

Para cada tema, se seguirá el siguiente orden a saber:

- Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real
- Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- Puntos débiles y amenazas.
- Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.
2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen al cambio propuesto.
4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

1. Hecho encontrado.
   - Ha de ser relevante para el auditor y para el cliente.
   - Ha de ser exacto, y además convincente.
   - No deben existir hechos repetidos.
2. Consecuencias del hecho.
   - Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.
3. Repercusión del hecho
   - Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.
4. Conclusión del hecho
   - No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.
5. Recomendación del auditor informático
   - Deberá entenderse por sí sola, por simple lectura.
   - Deberá estar suficientemente soportada en el propio texto.
   - Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
   - La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable

máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

7.16 ERRORES MÁS COMUNES EN LAS AUDITORÍAS DE CALIDAD

Cuando las Auditorías de la Calidad no producen ningún efecto, es probable que se hayan cometido errores que pueden poner en peligro su eficacia. En estos casos, conviene hacer un repaso de cuestiones de fondo, tales como:

- Analizar si el tipo de muestreo y la elección de la muestra no es el adecuado.
- Constatar la falta de asignación de prioridades a los problemas. Un síntoma es la excesiva profundización en los "muchos triviales". Los informes que llegan a la Dirección contienen excesivas recomendaciones.
- Comprobar la falta de formación, de los auditores y de los auditados, en el qué y el cómo se va a auditar y para qué sirven las auditorías.
- Averiguar si las condiciones excepcionales han sido tomadas como normales.
- Averiguar si el auditor tiene prejuicios, por los que emite observaciones subjetivas.

7.17. AUDITORÍA EN EL MARCO DE LOPD

7.17.1 Quién está obligado a la auditoría de la LOPD

Están obligadas a realizar la auditora de la LOPD todas aquellas organizaciones que, tratando datos de carácter personal traten datos de alguno de los siguientes tipos: sobre infracciones o sanciones, administrativas o penales (multas de tráfico, sanciones de Hacienda, etc.); que permitan obtener una evaluación de la personalidad del individuo (los típicos tests o encuestas, según los casos); los referentes a la ideología, religión, creencias, origen racial, salud o vida sexual (el dato de afiliación sindical para la confección de la nómina; los partes de baja o de alta del trabajador por motivos de salud, los datos médicos, etc.).

Es indiferente que los datos de que se trate lo estén en papel o en otro tipo de soporte, como el digital o informático.

7.17.2 Cada cuánto tiempo hay que hacerla

La LOPD indica que será una vez cada dos años, comenzándose a computar los mismos a partir de que se comenzaron a tratar dichos datos.

7.17.3 Quién la hace y a quién se le comunica

La LOPD da la opción de que la auditoría sea interna o externa, o sea, que la efectúe la misma organización, o bien se la encomiende a un tercero imparcial, deseablemente que se dedique profesionalmente a ello.

En realidad, la auditoría no hay que comunicarla a ningún sitio ni inscribirla en ningún registro. No obstante, sí hay obligación de conservar el documento en el que la misma se plasme, a fin de mostrarla al inspector correspondiente en el caso de ser inspeccionados por la Agencia Española de Protección de Datos.

7.17.4 Qué ocurre si no se hace

Se puede iniciar un procedimiento sancionador.

¿Cuáles son las sanciones?

La sanción que se impone por no cumplir a los requisitos y obligaciones de la LOPD varía entre 601,01 Euros y 601.012,10 Euros. Las infracciones son clasificadas en LEVES, GRAVES y MUY GRAVES.

Las sanciones que pueden suponer las infracciones son las siguientes:

- **Leves**: Multa de 601,01 € a 60.101,21€
- **Graves**: Multa de 60.101,21 € a 300.506,05 €
- **Muy Graves**: Multa de 300.506,05 € a 601.012,10 €

7.17.5 Qué contenido tiene la auditoría

Por un lado hay que indicar si la organización se adapta o no al reglamento, identificando (en caso de haberlos) los defectos encontrados, proponiendo cómo subsanarlos, e indicando en qué se basa todo lo anterior.

Por otro lado, el informe que contenga la auditoría habrá de ser analizado por el llamado Responsable de Seguridad (la persona que dentro de la organización está obligada a coordinar y controlar las medidas de seguridad, el cual dará traslado del mismo al Responsable de los Ficheros) quien decide acerca del contenido, uso y finalidad de los ficheros; es decir, el cliente que paga la auditoría o responsable de los datos a fin de que éste, estando ya informado del contenido de la misma, ordene adoptar las medidas necesarios en orden a la completa adaptación de su empresa a la LOPD.

7.17.6 Artículos relacionados con la auditoría en el marco de LOPD

- **Artículo 96**.- Auditoría.
  1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
  2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, 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 recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

- Tipos de ficheros
  1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas de **nivel básico**.
  2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por prestación de servicios de solvencia y crédito, deberán reunir, además de las medidas de nivel básico, las calificadas como de **nivel medio**.
  3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de **nivel alto**.
  4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de **nivel medio**.
  5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

7.17.2 Medidas en Reglamento LOPD

MEDIDAS DE NIVEL BÁSICO: Ficheros que contengan datos de carácter personal.

- Medidas de seguridad aplicables a ficheros y tratamientos automatizados.
  - Funciones y obligaciones del personal.
  - Registro de incidencias.
  - Control de acceso.
  - Gestión de soportes y documentos.
  - Identificación y autenticación.
  - Copias de respaldo y recuperación.
- Medidas de seguridad aplicables a ficheros y tratamientos no automatizados.
  - Obligaciones comunes.
  - Criterios de archivo.

- Dispositivos de almacenamiento.
- Custodia de los soportes.

MEDIDAS DE NIVEL MEDIO: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por prestación de servicios de solvencia y crédito.

- Medidas de seguridad aplicables a ficheros y tratamientos automatizados.
  - Responsable de seguridad.
  - Auditoría.
  - Gestión de soportes y documentos.
  - Identificación y autenticación.
  - Control de acceso físico.
  - Registro de incidencias.
- Medidas de seguridad aplicables a ficheros y tratamientos no automatizados.
  - Responsable de seguridad.
  - Auditoría.

MEDIDAS DE NIVEL ALTO: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

- Medidas de seguridad aplicables a ficheros y tratamientos automatizados.
  - Gestión y distribución de soportes.
  - Copias de respaldo y recuperación.
  - Registro de accesos.
  - Telecomunicaciones.
- Medidas de seguridad aplicables a ficheros y tratamientos no automatizados.
  - Almacenamiento de la información.
  - Copia o reproducción.
  - Acceso a la documentación.
  - Traslado de documentación.

CAPÍTULO 8: CRMR

8. CRMR

8.1 DEFINICIÓN DE LA METODOLOGÍA CRMR

CRMR son las siglas de Computer resource management review; su traducción más adecuada, Evaluación de la gestión de recursos informáticos. Esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio del management.

Una revisión de esta naturaleza no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios.

8.2 SUPUESTOS DE APLICACIÓN

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

8.3 ÁREAS DE APLICACIÓN

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en el punto anterior:

- Gestión de Datos.
- Control de Operaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

CRMR no es adecuado para evaluar la procedencia de adquisición de nuevos equipos (Capacity Planning) o para revisar muy a fondo los caminos críticos o las holguras de un Proyecto complejo.

8.4 OBJETIVOS

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos.

Las Recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijas responsabilidades.
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad.
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

8.5 ALCANCE

Se fijarán los límites que abarcará el CRMR, antes de comenzar el trabajo.

Se establecen tres clases:

- Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.
- Medio. En este caso, el CRMR ya establece conclusiones y Recomendaciones, tal y como se hace en la auditoría informática ordinaria.
- Amplio. El CRMR incluye Planes de Acción, aportando técnicas de implementación de las Recomendaciones, a la par que desarrolla las conclusiones.

8.6 INFORMACIÓN NECESARIA PARA LA EVALUACIÓN DEL CRMR

Se determinan en este punto los requisitos necesarios para que esta simbiosis de auditoría y consultoría pueda llevarse a cabo con éxito.

- El trabajo de campo del CRMR ha de realizarse completamente integrado en la estructura del Centro de Proceso de Datos del cliente, y con los recursos de éste.
- Se deberá cumplir un detallado programa de trabajo por tareas.
- El auditor-consultor recabará determinada información necesaria del cliente.

Se tratan a continuación los tres requisitos expuestos:

1. Integración del auditor en el Centro de Procesos de Datos a revisar

No debe olvidarse que se están evaluando actividades desde el punto de vista gerencial. El contacto permanente del auditor con el trabajo ordinario del Centro de Proceso de Datos permite a aquél determinar el tipo de esquema organizativo que se sigue.

2. Programa de trabajo clasificado por tareas

Todo trabajo habrá de ser descompuesto en tareas. Cada una de ellas se someterá a la siguiente sistemática:

- Identificación de la tarea.
- Descripción de la tarea.
- Descripción de la función de dirección cuando la tarea se realiza incorrectamente.
- Descripción de ventajas, sugerencias y beneficios que puede originar un cambio o modificación de tarea
- Test para la evaluación de la práctica directiva en relación con la tarea.
- Posibilidades de agrupación de tareas.
- Ajustes en función de las peculiaridades de un departamento concreto.
- Registro de resultados, conclusiones y Recomendaciones.

3. Información necesaria para la realización del CRMR

El cliente es el que facilita la información que el auditor contrastará con su trabajo de campo.

Se muestra a continuación una Checklist completa de los datos necesarios para confeccionar el CRMR:

- Datos de mantenimiento preventivo de Hardware.
- Informes de anomalías de los Sistemas.
- Procedimientos estándar de actualización.
- Procedimientos de emergencia.
- Monitorización de los Sistemas.
- Informes del rendimiento de los Sistemas.
- Mantenimiento de las Librerías de Programas.
- Gestión de Espacio en disco.
- Documentación de entrega de Aplicaciones a Explotación.
- Documentación de alta de cadenas en Explotación.
- Utilización de CPU, canales y discos.
- Datos de paginación de los Sistemas.
- Volumen total y libre de almacenamiento.
- Ocupación media de disco.
- Manuales de Procedimientos de Explotación.

8.7 CASO PRÁCTICO DE UNA AUDITORÍA DE SEGURIDAD INFORMÁTICA (CICLO DE SEGURIDAD)

A continuación, un caso de auditoría de área general para proporcionar una visión más desarrollada y amplia de la función auditora.

Es una auditoría de Seguridad Informática que tiene como misión revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más importantes de aquél.

8.7.1 Ciclo de Seguridad

El objetivo de esta auditoría de seguridad es revisar la situación y las cuotas de eficiencia de la misma en los órganos más importantes de la estructura informática.

Para ello, se fijan los supuestos de partida:

El área auditada es la Seguridad. El área a auditar se divide en: Segmentos.

Los segmentos se dividen en: Secciones.

Las secciones se dividen en: Subsecciones.

De este modo la auditoría se realizara en 3 niveles.

Los segmentos a auditar, son:

- Segmento 1: Seguridad de cumplimiento de normas y estándares.
- Segmento 2: Seguridad de Sistema Operativo.
- Segmento 3: Seguridad de Software.
- Segmento 4: Seguridad de Comunicaciones.
- Segmento 5: Seguridad de Base de Datos.
- Segmento 6: Seguridad de Proceso.
- Segmento 7: Seguridad de Aplicaciones.
- Segmento 8: Seguridad Física.

Se darán los resultados globales de todos los segmentos y se realizará un tratamiento exhaustivo del Segmento 8, a nivel de sección y subsección.

Conceptualmente la auditoría informática en general y la de Seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:

Fase 0. Causas de la realización del ciclo de seguridad.

Fase 1. Estrategia y logística del ciclo de seguridad.

Fase 2. Ponderación de sectores del ciclo de seguridad.

Fase 3. Operativa del ciclo de seguridad.

Fase 4. Cálculos y resultados del ciclo de seguridad.

Fase 5. Confección del informe del ciclo de seguridad.

A su vez, las actividades auditoras se realizan en el orden siguiente:

1. Comienzo del proyecto de Auditoría Informática.
2. Asignación del equipo auditor.
3. Asignación del equipo interlocutor del cliente.
4. Cumplimentación de formularios globales y parciales por parte del cliente.
5. Asignación de pesos técnicos por parte del equipo auditor.
6. Asignación de pesos políticos por parte del cliente.
7. Asignación de pesos finales a segmentos y secciones.
8. Preparación y confirmación de entrevistas.
9. Entrevistas, confrontaciones y análisis y repaso de documentación.
10. Cálculo y ponderación de subsecciones, secciones y segmentos.
11. Identificación de áreas mejorables.
12. Elección de las áreas de actuación prioritaria.
13. Preparación de recomendaciones y borrador de informe
14. Discusión de borrador con cliente.
15. Entrega del informe.

8.7.1.1 Fase 0: Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma.

El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad. Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costes, obligaciones legales, situación de ineficiencia global notoria, etc.

De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

8.7.1.2 Fase 1: Estrategia y Logística del Ciclo de Seguridad

Constituye la FASE 1 del ciclo de seguridad y se desarrolla en las actividades 1, 2 y 3:

1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente.
3. Cumplimentación de un formulario general por parte del cliente, para la realización del estudio inicial.

Con las razones por las cuales va a ser realizada la auditoría (Fase 0), el equipo auditor diseña el proyecto de Ciclo de Seguridad con arreglo a una estrategia definida en función del volumen y complejidad del trabajo a realizar, que constituye la Fase 1 del punto anterior.

Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de estos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los

mencionados recursos, determina a su vez la eficiencia y la economía del Proyecto.

Los planes del equipo auditor se desarrollan de la siguiente manera:

1. Eligiendo el responsable de la auditoría su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.
2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.
3. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.

Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad.

8.7.1.3 Fase 2: Ponderación de Sectores del Ciclo de Seguridad

Esta constituye la Fase 2 del Proyecto y engloba las siguientes actividades:

1. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
2. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
3. Asignación de pesos finales a los Segmentos y Secciones. El peso final es el promedio del peso técnico y del peso político. Las Subsecciones se calculan pero no se ponderan.

Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.

Las asignaciones de pesos a Secciones y Segmentos del área de seguridad que se audita, se realizan del siguiente modo:

8.7.1.3.1 Pesos Técnicos

Son los coeficientes que el equipo auditor asigna a los Segmentos y a las Secciones.

8.7.1.3.2 Pesos Políticos

Son los coeficientes o pesos que el cliente concede a cada Segmento y a cada Sección del Ciclo de Seguridad.

Ciclo de Seguridad. Suma Pesos Segmentos = 100 *(con independencia del número de segmentos consideradas)*			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12
Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
TOTAL	**100**	**100**	**100**

Tabla 7: Ciclo de seguridad

8.7.1.3.3 Pesos Finales

Son el promedio de los pesos anteriores.

El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos.

Suma Peso Secciones = 20 *(con independencia del número de Secciones consideradas)*			
Secciones	**Pesos Técnicos**	**Pesos Políticos**	**Pesos Finales**
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Tabla 8: Pesos finales

Puede observarse la diferente apreciación de pesos por parte del cliente y del equipo auditor. Mientras éstos estiman que las Normas y Estándares y los Procesos son muy importantes, el cliente no los considera tanto, a la vez que prima, tal vez excesivamente, el Software Básico.

Del mismo modo, se concede a todos los segmentos el mismo valor total que se desee, por ejemplo 20, con absoluta independencia del número de Secciones que tenga cada Segmento.

En este caso, se han definido y pesado cinco Secciones del Segmento de Seguridad Física.

Cabe aclarar, sólo se desarrolló un solo Segmento a modo de ejemplo.

8.7.1.4 Fase 3: Operativa del Ciclo de Seguridad

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

- Preparación y confirmación de entrevistas.
- Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud.

El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado. Si esta no se produce, el responsable lo hará saber al cliente.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos.

El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

La entrevista concreta suele abarcar Subsecciones de una misma Sección tal vez una sección completa. Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s. Debe identificarse quien ha dicho qué, si son más de una las personas entrevistadas.

Las Checklist's son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y verificar los resultados de las pruebas auditoras.

La evaluación de las Checklists, las pruebas realizadas, la información

facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoría, que se materializarán en el informe final.

A continuación, un ejemplo de auditoría de la Sección de Control de Accesos del Segmento de Seguridad Física:

Vamos a dividir a la Sección de Control de Accesos en cuatro Subsecciones:

1. Autorizaciones
2. Controles Automáticos
3. Vigilancia
4. Registros

En las siguientes Checklists, las respuestas se calificarán de 1 a 5, siendo1 la más deficiente y 5 la máxima puntuación.

Control de Accesos: **Autorizaciones**		
Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Explotación, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuáles son las personas autorizadas?	El personal de vigilancia y el Jefe de Explotación.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se prevén las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
TOTAL AUTORIZACIONES		**24/30** **80%**

Tabla 9: Control de accesos: Autorizaciones

Control de Accesos: **Controles Automáticos**		
Preguntas	Respuestas	Puntos
¿Cree Ud. que los Controles Automáticos son adecuados?	Si, aunque ha de reconocerse que a pie puede llegarse por la noche hasta el edificio principal.	3
¿Quedan registradas todas las entradas y salidas del Centro de Cálculo?	No, solamente las del personal ajeno a Operación.	3
Al final de cada turno, ¿Se controla el número de entradas y salidas del personal de Operación?	Sí, y los vigilantes los verifican.	5
¿Puede salirse del Centro de Cálculo sin tarjeta magnética?	Sí, porque existe otra puerta de emergencia que puede abrirse desde adentro	3
TOTAL CONTROLES AUTOMATICOS		**14/20** **70%**

Tabla 10: Control de accesos: Controles Automáticos

Control de Accesos: **Vigilancia**		
Preguntas	Respuestas	Puntos
¿Hay vigilantes las 24 horas?	Sí.	5
¿Existen circuitos cerrados de TV exteriores?	Sí.	5
Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?	No.	2
¿Conocen los vigilantes los terminales que deben quedar encendidos por la noche?	No, sería muy complicado.	2
TOTAL VIGILANCIA		**14/20** **70%**

Tabla 11: Control de accesos: Vigilancia

Control de Accesos: **Registros**		
Preguntas	Respuestas	Puntos
¿Existe una adecuada política de registros?	No, reconocemos que casi nunca, pero hasta ahora no ha habido necesidad.	1
¿Se ha registrado alguna vez a una persona?	Nunca.	1
¿Se abren todos los paquetes dirigidos a personas concretas y no a Informática?	Casi nunca.	1
¿Hay un cuarto para abrir los paquetes?	Sí, pero no se usa siempre.	3
TOTAL REGISTROS		**6/20** **30%**

Tabla 12: Control de accesos: Registros

8.7.1.5 Fase 4: Cálculos y Resultados del Ciclo de Seguridad

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad.

A continuación se describen las áreas de esta fase.

- Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, sólo se calculan.
- Identificación de materias mejorables.
- Priorización de mejoras.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Sólo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes.

Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:

- Autorizaciones 80%
- Controles Automáticos 70%
- Vigilancia 70%
- Registros 30%

Promedio de Control de Accesos 62,5%

Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.

Prosiguiendo con el ejemplo, se procedió a la evaluación de las otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad: Segmento 8, Seguridad Física.		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Tabla 13: Ciclo de Seguridad: Segmento 8, seguridad Física

Conocidas los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:

Seg. 8 = PromedioSección1 * peso + PromedioSecc2 * peso + PromSecc3 * peso + PromSecc4 * peso + PromSecc5 * peso / (peso1 + peso2 + peso3 + peso4 + peso5)

Ó

Seg. 8 = (57,5 * 6) + (62,5 * 4) + (70 * 5) + (52,5 * 3) + (47,2 * 2) / 20

Seg. 8 = 59,85%

A continuación, la evaluación final de los demás Segmentos del ciclo de Seguridad Sistemática seguida para el cálculo y evaluación del Ciclo de Seguridad:

Ciclo de Seguridad. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
Promedio Total Área de Seguridad	**100**	**63,3%**

Tabla 14: Ciclo de Seguridad: Evaluación y pesos de Segmentos

- Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.
- Cálculo matemático de todas las subsecciones de cada sección, como media aritmética de las preguntas específicas.
- Cálculo matemático de la Sección, como media aritmética de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
- Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.
- Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Finalmente, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero los Segmentos, luego las Secciones y por último las Subsecciones. En todos los casos se referenciarán respecto a tres zonas: roja, amarilla y verde.

La zona roja corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del Informe como en la toma de medidas para la corrección.

La zona amarilla corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja.

La zona verde requiere solamente alguna acción de mantenimiento a largo plazo.

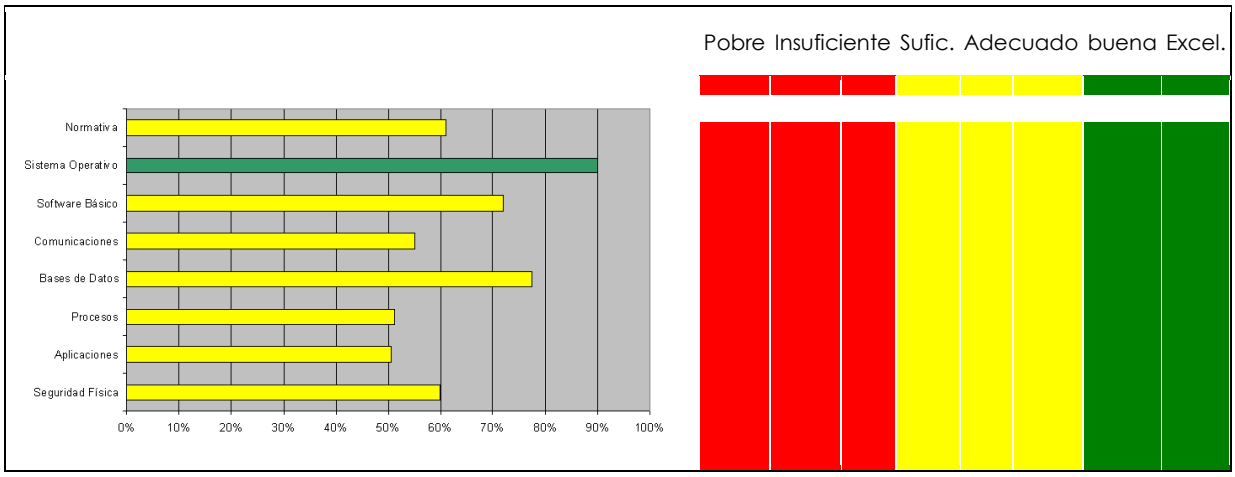


Imagen 6: Gráfico de barras: Segmentos, secciones y subsecciones

8.7.1.6 Fase 5: Confección del informe del Ciclo de Seguridad

La fase 5 comprende los siguientes puntos a realizar:

- Preparación de borrador de informe y Recomendaciones.
- Discusión del borrador con el cliente.
- Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Esta acta se incorporará al Informe Final.

Las Recomendaciones del Informe son de tres tipos:

- Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.
- Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.
- Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

CAPÍTULO 9: ALGUNAS VULNERABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

9. ALGUNAS VULNERABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

9.1 LAS VEINTE VULNERABILIDADES MÁS IMPORTANTES EN INTERNET

The SANS Institute (System Administration, Networking, and Security Institute) y el FBI, han venido publicando una extensa lista con las veinte vulnerabilidades más explotadas en la mayoría de los ataques a sistemas computacionales vía Internet.

Recientemente, se ha publicado una actualización de su versión original (en inglés). El listado completo, incluye soluciones y sugerencias de cada vulnerabilidad.

Estos 20 artículos incluyen conocidas vulnerabilidades tanto en Windows, como en Unix, las que son explotadas a menudo por atacantes y programas malévolos, como virus y troyanos.

Rasgos de seguridad más comunes

Entre los errores de seguridad más comunes, está el de instalar cualquier software del sistema sin quitar los servicios innecesarios, ni instalar todos los parches de seguridad recomendados.

También la falta de contraseñas, o el uso de estas con pocos caracteres, es un problema de seguridad enorme para cualquier corporación. También deberían evitarse las contraseñas predefinidas o por defecto.

Demasiados puertos abiertos para que algún usuario pueda conectarse a su ordenador es contraproducente. Las recomendaciones obvias son cerrar todos los puertos y luego sólo abrir los que realmente se necesiten.

Medidas de Seguridad elementales

Utilizar contraseñas más fuertes. Escoger aquellas que sean difíciles o imposibles de suponer.

Poner contraseñas diferentes a cada una de las cuentas. Realizar respaldos regulares de datos críticos. Estos respaldos deben hacerse por lo menos una vez al día en el caso de usuarios o empresas pequeñas. Para organizaciones más grandes y complejas, deben realizarse respaldos completos por lo menos una vez a la semana, y respaldos incrementales todos los días.

Utilizar un antivirus monitoreando toda actividad de archivos, actualizándolo periódicamente (sugerido una vez a la semana, lo ideal es diariamente).

Utilizar cortafuegos como barrera entre su ordenador e Internet. Los cortafuegos normalmente son productos de software. Ellos son esenciales para aquellos que poseen enlaces de banda ancha con conexiones las 24 horas (DSL, cable módem, etc.), y muy recomendados para todos los que utilicen Internet, aún a través de la línea telefónica.

No dejar que los ordenadores sigan ON-LINE cuando no están en uso.

No abrir bajo ningún concepto, adjuntos en el correo electrónico que venga de extraños, sin importar lo que mencione su asunto o el archivo adjunto. Sospechar siempre de cualquier adjunto de alguien conocido, que le envía un adjunto que no se solicitó.

Bajar e instalar regularmente los parches necesarios a medida que estos vayan apareciendo.

En concreto, estas pocas vulnerabilidades son la base de la mayoría de los

ataques exitosos, que suelen aprovecharse de las brechas más conocidas con las herramientas de ataque más efectivas y fáciles de conseguir. La mayoría de los atacantes, simplemente se aprovecha de quienes no actualizan su software, casi siempre por pereza.

Según el FBI y SANS, la oportuna instalación de parches largamente anunciados, hubiera prevenido la mayoría de los ataques exitosos.

Vulnerabilidades que afectan a todos los sistemas

1. Instalaciones por defecto de sistemas y aplicaciones

La mayoría del software, incluyendo sistemas operativos y aplicaciones, viene con scripts de instalación o programas de instalación. La meta de estos programas de instalación es dejar los sistemas operativos lo más rápido posible, con la mayor parte de funciones disponibles o habilitadas, y con la ayuda de muy poco trabajo por parte del administrador. Para lograr esta meta, los scripts típicamente instalan más componentes de los que se necesitan en realidad. La filosofía de los fabricantes es que resulta mejor habilitar funciones que no son utilizadas que hacer que el usuario instale funciones adicionales a medida que las vaya requiriendo. Esta aproximación, aunque conveniente para el usuario, genera la mayoría de las vulnerabilidades de seguridad debido a que los usuarios no mantienen activamente o aplican los parches a los componentes de software que utilizan. Más aún, muchos usuarios no son conscientes de lo que está realmente instalado en sus propios sistemas, dejando peligrosos programas de demostración en ellos por el simple hecho de que no saben que están ahí.

Aquellos servicios a los que no se les han aplicado los parches proveen rutas para que los atacantes puedan tomar el control de las máquinas.

Con respecto a los sistemas operativos, las instalaciones por defecto casi siempre incluyen extraños servicios con sus correspondientes puertos abiertos. Los atacantes se introducen en estos sistemas por medio de dichos puertos. En la mayoría de los casos, cuantos menos puertos se hallen abiertos, menos alternativas tiene un atacante para comprometer su red. Con respecto a las aplicaciones, las instalaciones por defecto usualmente incluyen programas o scripts de demostración que no son realmente necesarios. Una de las vulnerabilidades más serias en los servidores Web son los scripts de ejemplo; los atacantes usan estos scripts para comprometer el sistema u obtener información acerca de éste. En la mayoría de los casos el administrador del sistema comprometido no se dio cuenta siquiera de que estos scripts de ejemplo se encontraban instalados. Los scripts de ejemplo son un problema porque por lo general no son sometidos al mismo proceso de control de calidad que otros programas. La revisión de errores es habitualmente olvidada por lo que ofrecen un terreno abonado para ataques del tipo desbordamiento de buffer.

2. Cuentas sin contraseña o contraseñas débiles

La mayoría de los sistemas se encuentran configurados para usar contraseñas secretas como primera y única línea de defensa. Los nombres de usuario (user IDs) son relativamente fáciles de conseguir y la mayoría de las compañías tienen accesos telefónicos que se saltan el cortafuegos. Es por esto que si un atacante puede determinar el nombre de una cuenta y su contraseña correspondiente, él o ella pueden entrar en la red. Dos grandes problemas lo constituyen las contraseñas fáciles de adivinar y las contraseñas por defecto, pero aún así, uno mucho mayor son las cuentas sin contraseña.

Adicionalmente, muchos sistemas contienen cuentas que vienen incluidas o cuentas por defecto. Estas cuentas generalmente tienen la misma contraseña para todas las instalaciones del software. Los atacantes habitualmente buscan estas

cuentas ya que son bien conocidas por su comunidad. Por esta razón, cualquier cuenta preexistente o por defecto, debe ser identificada y eliminada del sistema.

Resulta afectado cualquier sistema operativo o aplicación en los cuales los usuarios se autentifiquen por medio de un nombre de usuario y una contraseña.

3. Respaldos (backups) incompletos o inexistentes

Cuando ocurre un incidente (y va a ocurrir en casi todas las organizaciones), la recuperación requiere respaldos actualizados y métodos probados para restaurar la información. Algunas organizaciones hacen respaldos diarios, pero nunca verifican que éstos se encuentren realmente funcionando. Otros definen políticas de respaldo, pero no políticas o procedimientos de restauración. Tales errores son usualmente descubiertos después de que un atacante ha entrado en los sistemas y ha destruido o arruinado la información.

Un segundo problema que afecta a los respaldos es la insuficiente protección física del medio de respaldo. Los respaldos contienen la misma información sensible que reside en los servidores, y debe, por lo tanto, ser protegido de la misma forma.

Los respaldos deben ser realizados al menos diariamente. El requerimiento mínimo en la mayoría de las organizaciones es realizar un respaldo completo una vez a la semana y respaldos incrementales todos los días. Debe verificarse al menos una vez al mes el soporte del respaldo mediante la restauración en un servidor de prueba que permita ver si la información se está respaldando correctamente. Este es el requerimiento mínimo. La mejor solución de respaldo es uno total y redundante a prueba de fallos (failover) - una solución que es requerida para sistemas financieros y de comercio electrónico críticos y de tiempo real, sistemas que controlan infraestructura crítica y algunos sistemas del Departamento de Defensa.

4. Gran número de puertos abiertos

Tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente. El resto de los puertos deben ser cerrados.

5. Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas

La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima.

6. Registro de eventos (logging) incompleto o inexistente

Una de las máximas de la seguridad es, "la prevención es ideal, pero la detección es fundamental". Mientras usted permita fluir el tráfico entre su red e Internet, la probabilidad de que un atacante llegue silenciosamente y penetre está siempre latente. Cada semana se descubren nuevas vulnerabilidades y existen muy pocas formas de defenderse de los ataques que hagan uso de las mismas. Una vez que usted ha sido atacado, sin registros (logs) hay muy pocas probabilidades de que descubra qué hicieron realmente los atacantes. Sin esa información su organización debe elegir entre recargar completamente el sistema operativo desde el soporte original y luego esperar que los respaldos se encuentren en buenas condiciones, o bien correr y asumir el riesgo que representa seguir utilizando un sistema que un atacante controla.

Usted no puede detectar un ataque si no sabe qué está ocurriendo en la red. Los registros le proporcionan los detalles de lo que está ocurriendo, qué sistemas se encuentran bajo ataque y qué sistemas han sido comprometidos.

El registro debe ser realizado de forma regular sobre todos los sistemas clave, y

deben ser archivados y respaldados porque nunca se sabe cuándo se pueden necesitar. La mayoría de los expertos recomiendan enviar todos los registros a un recolector central que escribe la información en un soporte que sólo admita una escritura, con el fin de que el atacante no pueda sobrescribir los registros para evitar la detección.

7. Programas CGI vulnerables

La mayoría de los servidores Web, permiten el uso de programas CGI (Common Gateway Interface) para proporcionar interactividad a las páginas web, habilitando funciones tales como recolección de información y verificación. De hecho, la mayoría de los servidores web vienen con programas CGI de ejemplo preinstalados. Desgraciadamente demasiados programadores de CGIs pasan por alto el hecho de que sus programas proporcionan un vínculo directo entre cualquier usuario en cualquier parte de Internet y el sistema operativo en la máquina que se encuentra ejecutando el servidor Web. Los programas CGI vulnerables resultan especialmente atractivos para los intrusos ya que son relativamente fáciles de localizar y de operar con los mismos privilegios y poder que tiene el software del servidor Web. Es de sobra conocido el hecho de que los intrusos abusan de los programas CGI para modificar páginas Web, robar información de tarjetas de crédito e instalar puertas traseras que les servirán para posteriormente tener acceso a los sistemas comprometidos. Las aplicaciones en los servidores web son igualmente vulnerables a amenazas creadas por programadores descuidados o no muy bien instruidos. Como regla general, los programas de ejemplo deben ser siempre eliminados de los sistemas de producción.

Vulnerabilidades más críticas en sistemas Windows

8. Vulnerabilidad Unicode (Salto de directorio en servidores Web - Web Server Folder Traversal)

Unicode proporciona un número único para cada carácter, sin importar cuál sea la plataforma, cuál sea el programa o cuál sea el lenguaje. El estándar Unicode ha sido adoptado por la mayoría de los fabricantes. Mediante el envío a un servidor IIS de una URL creada cuidadosamente con secuencias inválidas de Unicode UTF-8, un atacante puede forzar a que el servidor literalmente entre y salga de cualquier directorio y ejecute scripts de forma arbitraria. Este tipo de ataque es conocido como el ataque de salto de directorio (Directory Traversal Attack).

IIS no fue escrito ni diseñado para realizar un chequeo de seguridad en secuencias de sobredimensión. Por esta razón, si se envía una secuencia sobredimensionada de Unicode en una URL se evitan los chequeos de seguridad de Microsoft. Si la petición se realiza desde un directorio marcado como ejecutable, el atacante puede ejecutar los archivos ejecutables en el servidor.

9. Desbordamiento de Buffer en extensiones ISAPI

ISAPI, que significa Interfaz de Programación de Aplicaciones para Servicios de Internet, permite que los programadores puedan extender las capacidades de un servidor mediante el uso de DLLs. Varias de las DLLs, como idq.dll, contienen errores de programación que causan que éstas realicen un chequeo incorrecto de límites. En particular no bloquean entradas inaceptablemente largas. Los atacantes pueden enviar información a estas DLLs, en lo que se conoce como un ataque por desbordamiento de buffer, y tomar control de un servidor IIS.

10. Exploit para RDS del IIS (Servicios de información remota Microsoft)

Es posible explotar fallos de programación en los servicios RDS de IIS con el fin de ejecutar comandos remotos con atributos administrativos.

11. NETBIOS - recursos compartidos en red no protegidos

El protocolo SMB (Server Message Block), también conocido como CIFS (Common Internet File System), permite habilitar la compartición de recursos a través de la red. Muchos usuarios permiten el acceso a sus discos con la intención de facilitar el trabajo en grupo con sus colaboradores. Sin saberlo, están abriendo sus sistemas a cualquier atacante al permitir el acceso, tanto de lectura como de escritura, a otros usuarios de la red.

Habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez. Las máquinas Macintosh y UNIX son también vulnerables a ataques de este tipo si los usuarios habilitan la compartición de archivos.

12. Fuga de información a través de conexiones de tipo "sesión nula"

Una conexión de tipo "sesión nula", también conocida como "entrada anónima al sistema", es un mecanismo que permite a un usuario anónimo obtener información a través de la red, o conectarse sin autenticarse contra el sistema. La cuenta SYSTEM se usa para diversas tareas críticas del sistema. Cuando una máquina necesita obtener datos de sistema de otra, la cuenta SYSTEM abrirá una "sesión nula" contra la otra máquina. Dado que no es posible conectarse a otros sistemas utilizando un identificador de usuario y una contraseña, utiliza una "sesión nula" para obtener acceso. Desgraciadamente, un atacante también puede utilizar la "sesión nula" del mismo modo.

13. Hashing débil en SAM (LM hash)

Dado que LAN Manager utiliza un esquema de cifrado mucho más débil que el resto de los utilizados por Microsoft, las contraseñas LAN Manager pueden ser descifradas en un corto espacio de tiempo. Incluso aquellas contraseñas más robustas pueden ser descifradas en menos de un mes.

Vulnerabilidades más críticas en sistemas Unix

14. Desbordamiento de Buffer en los servicios RPC

Las llamadas a procedimiento remoto (RPCs) hacen posible que programas que se encuentran ejecutándose en un sistema ejecuten a su vez otros programas en un segundo sistema. Este tipo se servicios son ampliamente utilizados para acceder a servicios de red tales como el compartir archivos a través de NFS o NIS. Un gran número de vulnerabilidades causadas por defectos en los RPC han sido activamente explotadas.

15. Vulnerabilidades en sendmail

Sendmail es un programa que envía, recibe y redirecciona la mayor parte del correo electrónico procesado en máquinas UNIX y Linux. Lo extendido de su uso en Internet lo convierte en uno de los objetivos prioritarios de los crackers. A lo largo de los años han sido descubiertos en sendmail diversos defectos. En uno de los ataques más habituales, el atacante envía un mensaje falsificado a la máquina que está ejecutando sendmail, éste lee el mensaje y lo interpreta como un conjunto de instrucciones mediante las cuales la máquina víctima envía su archivo de contraseñas a la máquina del atacante (o a otra víctima) donde las contraseñas pueden ser descifradas.

16. Debilidades en BIND

El paquete Berkeley Internet Name Domain (BIND) es una de las implementaciones más utilizadas del Servicio de Nombres de Dominio (DNS) - el importante sistema que nos permite localizar los sistemas en Internet por su nombre sin necesidad de utilizar direcciones IP - lo que la convierte en uno de los blancos

favoritos para los crackers. Versiones obsoletas de BIND pueden también ser vulnerables a ataques de desbordamiento de buffer que los crackers pueden utilizar para obtener acceso no autorizado.

17. Los comandos "r"

Las relaciones de confianza son ampliamente utilizadas en el mundo UNIX, especialmente para la administración de sistemas. Las empresas habitualmente asignan a un único administrador la responsabilidad sobre docenas o incluso centenares de sistemas. Los administradores a menudo utilizan relaciones de confianza a través del uso de los comandos "r" para poder saltar de sistema en sistema convenientemente. Los comandos "r" permiten acceder a sistemas remotos sin tener que introducir ninguna contraseña. En lugar de solicitar un nombre de usuario y su contraseña asociada, la máquina remota autentifica a cualquiera que provenga de direcciones IP "amigas". Si un atacante consigue el control de cualquier máquina en una red en la que confiamos, él o ella pueden acceder al resto de las máquinas que confían en la máquina comprometida.

18. LPD (demonio del protocolo de impresión remota)

En UNIX, el demonio "in.lpd" proporciona los servicios necesarios para que los usuarios puedan hacer uso de la impresora local. LPD espera dichas peticiones escuchando en el puerto TCP 515. Los programadores que desarrollaron el código que transfiere trabajos de impresión de una máquina a otra, cometieron un error que se ha traducido en una vulnerabilidad de desbordamiento de buffer. Si el demonio recibe demasiados trabajos de impresión en un corto intervalo de tiempo, éste morirá o permitirá la ejecución de código arbitrario con privilegios elevados.

19. Sadmind y Mountd

Sadmind permite la administración remota de sistemas Solaris, proporcionando un interfaz gráfico para labores de administración de sistemas. Mountd, por otro lado, controla y arbitra el acceso a los volúmenes NFS en los sistemas UNIX. Debido a errores de programación cometidos por los desarrolladores de estas aplicaciones, existe la posibilidad de utilizar desbordamientos de buffer en las mismas para conseguir acceso como super-usuario en los sistemas afectados.

20. Nombres de comunidad SNMP por omisión

El Protocolo Simple de Administración de Red (Simple Network Management Protocol - SNMP) es ampliamente utilizado por los administradores de red para supervisar y administrar todo tipo de dispositivos de red, desde enrutadores hasta impresoras u ordenadores. El único mecanismo de autenticación que SNMP usa es un "nombre de comunidad" no cifrado. Si la falta de encriptación ya de por sí es mala, peor aún es que la mayor parte de los dispositivos SNMP utilicen como nombre de comunidad por omisión la palabra "public". Los posibles agresores pueden utilizar esta vulnerabilidad en SNMP para reconfigurar o incluso desactivar dispositivos remotamente. La captura del tráfico SNMP, por otra parte, puede revelar una gran cantidad de información sobre la estructura de la red, así como de los dispositivos y sistemas conectados a la misma. Toda esa información puede ser utilizada por parte de los intrusos para seleccionar blancos y planear ataques. SNMP no es exclusivo del mundo UNIX. Pero la mayor parte de los ataques de esta índole se producen contra sistemas UNIX debido a configuraciones SNMP deficientes.

9.2 CONCEPTO DE NEUTRALIDAD DE RED

Un nuevo concepto se pone de moda en el sector de las telecomunicaciones: la "net neutrality" (NN o neutralidad de red).

La neutralidad de la red significa, que todo contenido de Internet se debe tratar del mismo modo y moverse a la misma velocidad por la red.

Es un acuerdo implícito desde el nacimiento de la red en la cual todos los proveedores tratan de la misma forma a todos los sitios.

En realidad, como concepto no introduce nada nuevo a lo ya conocido, dado que su significado puede asociarse perfectamente al tradicional "principio de no discriminación".

Este principio, puede definirse como la igualdad en el tratamiento que debe dársele al tráfico que circula por Internet, con independencia del contenido específico (que es transmitido de extremo a extremo) y de quien lo emita o lo reciba.

Se caracteriza por una arquitectura abierta y descentralizada, donde el control y la inteligencia de la red se circunscriben a las aplicaciones. Esto significa que el comportamiento del tráfico de paquetes de información por Internet es de libre circulación, y no responde a ningún tipo de restricción o condicionante.

El principio de neutralidad en la red establece que ésta debe operarse bajo tres principios: no discriminación, interconexión y acceso.

- El principio de *no* discriminación establece que todo el tráfico será tratado por igual a lo largo de la red.
- El principio de interconexión implica que el operador de cada red tiene el derecho y el deber de conectarse a cualquier otra red de Internet.
- El principio de acceso hace referencia al derecho que tienen los usuarios finales para establecer comunicaciones con otros usuarios finales en igualdad de condiciones, es decir, a establecer conexiones de igual a igual.

Se trata del proyecto de ley aprobado por el comité responsable de la legislación de las telecomunicaciones y que ha pasado de afirmar que los proveedores de banda ancha no podrán bloquear, deteriorar o interferir sin razón el acceso a Internet a su versión final en el que no hace defensa alguna de la neutralidad de la red y apenas deja un resquicio a la esperanza dejando que la Federal Communications Commission establezca las reglas.

En conclusión, podemos decir, que es el principio que establece que todo el tráfico que circula por Internet debe ser tratado en condiciones de igualdad, al margen de cuál sea el contenido y quiénes sean el emisor y el receptor.

9.2.1 <u>Desarrollo Histórico</u>

La evolución del sector de las telecomunicaciones está marcada por dos hitos temporales muy diferenciados:

- Hasta la década de los 90: el sector de las Telecomunicaciones se caracteriza por ser un mercado estable, fuertemente intervenido, basado fundamentalmente en el servicio telefónico fijo y con importantes economías de escala.
- A partir de los 90: el mercado se ve alterado por los procesos de desregularización, la aparición de nuevas tecnologías, el desarrollo de Internet y la explosión de los servicios móviles.

Cuando empezó, los expertos dijeron que todo el mundo tendría un e-mail, que la Red sería la mayor casa de subastas del mundo y que los teléfonos podrían acceder a versiones reducidas de la World Wide Web. No imaginaron hasta qué punto Internet cambiaría el modo en que vivimos, trabajamos y nos relacionamos.

Internet ha constituido sin lugar a dudas uno de los principales dinamizadores del sector de Telecomunicaciones. Sus orígenes se remontan a finales de la década de los 60, y en menos de 40 años ha registrado una evolución realmente espectacular.

Internet tuvo un origen público, esencialmente militar y académico, pero sólo a partir de su privatización y comercialización, a principios de los 90, inició su proceso de expansión, que no ha hecho más que acelerarse desde entonces en una espiral continua de innovación e implantación de proporciones históricamente desconocidas.

Internet se ha caracterizado desde su nacimiento por una arquitectura abierta y descentralizada, donde el control y la inteligencia de la red se circunscriben a las aplicaciones.

Este principio, que ha regido la Red hasta el presente, se conoce con el nombre de Net neutrality.

A la hora de diseñar la estructura de Internet se optó, por un modelo descentralizado, pensando, entre otras razones, que así sería más flexible y adaptable a su futura e imprevisible evolución posterior. Ello suponía, en la práctica, que en Internet la inteligencia estaría en las aplicaciones (periferia) y no en los routers (centro). Es lo que se denomina estructura end to end (e2e) o punto a punto.

Ello significa que el comportamiento del tráfico de paquetes de información por Internet es de libre circulación, y no responde a ningún tipo de restricción o condicionante: Internet no prioriza o da ventajas a unos servicios en función de otros. La selección y éxito de cada servicio/aplicación/contenido depende de la decisión del usuario final y no de las prioridades que establezcan los gestores de las infraestructuras de la red de forma particular.

Las protecciones que garantizaban la neutralidad de red han sido ley desde el nacimiento de Internet. Hasta el año pasado, cuando la Comisión Federal de Comunicaciones eliminó las normas que impedían a las empresas de cable y teléfono hacer discriminaciones entre los proveedores de contenido.

No obstante, la madurez alcanzada por la Red se materializa en nuevos retos, nuevas oportunidades y nuevos riesgos que han impulsado la aparición de posturas que defienden un cambio de filosofía hacia una red menos pública y controlada de forma centralizada.

Este cambio de filosofía ha sido liderado por las compañías de telecomunicaciones en su afán de adaptar su negocio al nuevo contexto en el que se encuentra Internet: creciente uso de la Voz sobre IP (VoIP); progresivo incremento en el uso de aplicaciones que requieren gran ancho de banda (juegos online, descargas de música y video…); mejoras en la tecnología de la Red que hacen más eficiente la provisión de servicio de banda ancha y abaratan el acceso al mismo; tendencia de algunos países (Corea del Sur, Francia) de crear sus propias redes de alta velocidad y de algunas ciudades de construir sus propias redes wireless; incremento de redes inalámbricas en el segmento residencial que permiten a los usuarios finales compartir conexiones a Internet, y por lo tanto, reducen los ingresos de los proveedores de telecomunicaciones…

Estos primeros escarceos en el cambio de concepción de Internet, una red que ha alcanzado impensables implicaciones sociales, tecnológicas y comerciales, han generado una gran controversia, inicialmente exclusiva a Estados Unidos, y que poco a poco se ha extendido a Europa. La audiencia celebrada por la Comisión de Comercio, Ciencia y Transporte del Senado de Estados Unidos ha situado ante la opinión pública un debate reducido anteriormente a círculos restringidos: ¿la Net neutrality debe plasmarse como principio legal o permanecer como realidad de facto de la arquitectura de Internet, como viene ocurriendo hasta ahora? La idea que subyace bajo este dilema es la propuesta de las principales proveedoras de banda ancha de EE.UU. de crear una segunda Internet más rápida para aquellos que paguen más.

Las empresas proveedoras de contenidos de Internet han visto amenazado su negocio y han cuestionado la viabilidad futura de Internet. Así pues, la respuesta de estas empresas ha sido la de plantear la Net neutrality como un principio legal (con validez jurídica) y que deje de ser simplemente una realidad de facto en Internet. Saben que, con ello, lograrían que los operadores de redes se constituyesen como transportistas neutrales del contenido en Internet, permitiendo que los consumidores puedan acceder libremente a ellos.

Empresas como Microsoft y Google respaldan la visión de una Red neutral, y se han pronunciado a favor de leyes que garanticen ese sistema. Sin embargo empresas de telecomunicaciones estadounidenses defienden un sistema de dos niveles en el que los datos de compañías e instituciones que pueden pagar aranceles tendrán prioridad sobre los que no están dispuestos a hacerlo.

El debate de la NN en el Senado de los Estados Unidos está suscitando numerosas audiencias -celebradas por la Comisión de Comercio, Ciencia y Transporte- en las que se ven enfrentadas las posiciones de las empresas con presencia en Internet (principalmente, las proveedoras de contenidos) y las de empresas que operan redes (la industria del cable y de telefonía).

Después de un intenso debate, la Cámara de Representantes estadounidense ha decidido rechazar el concepto de neutralidad de la Red, vigente desde el mismo nacimiento de Internet y que establece que todos los sitios deben ser tratados de igual manera por las compañías de telecomunicaciones que suministran el acceso a la Red.

9.2.2 Diferentes Posturas

Se distinguen los siguientes agentes participantes en el mercado de Internet: los proveedores de contenidos y/o servicios, los creadores de la infraestructura de red (proveedores de acceso a Internet), los proveedores de servicios de banda ancha (operadores de red u operadores de telecomunicaciones y cable) y los usuarios finales. Además, en el mercado de Internet, las entidades regulatorias juegan un importante papel al interaccionar de forma directa o indirecta con estos actores. Las diferentes posturas de cada uno de los colectivos atienden tanto a ventajas y desventajas inherentes a la estructura de cada uno de los modelos (Net neutrality y Non Net neutrality), como a beneficios y perjuicios derivados de los modelos de negocio a ellos asociados.

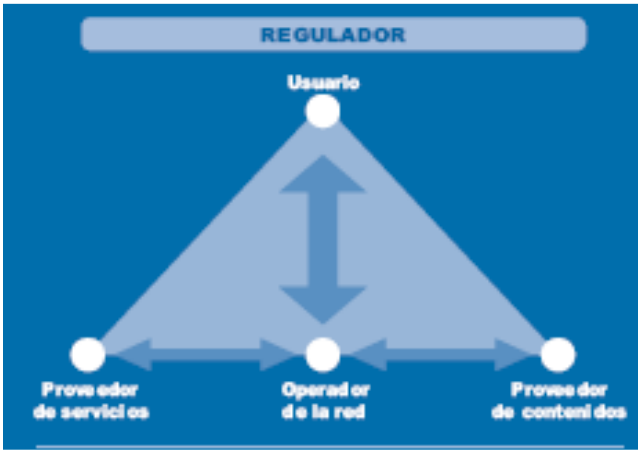


Imagen 7: Diferentes posturas

- **Proveedores de contenidos y/o servicios**

Dentro de este grupo se incluyen los proveedores de contenidos, servicios y aplicaciones de búsquedas, ISP, comercio electrónico y otras empresas de Internet. Algunos de los nombres que han saltado a la palestra dentro de este debate han sido tales como Amazon, EarthLink, eBay, Google, Microsoft, Skype, Sony, Vonag y Yahoo!, todos ellos a favor de una legislación que dé soporte a la Net neutrality.

- **Operadores de telecomunicaciones**

Entre las operadoras de telecomunicaciones que han centrado el debate en EE.UU. acerca de la Net neutrality destacan AT&T, Bell-South, Qwest, Versión, Comcast y RBOC. Todas ellas se posicionan en contra de una legislación sobre la neutralidad de la Red.

- **Operadores de cable**

Las compañías de cable como Cablevisión, COMSAT, Cox Communications o Time Warner Cable no se han posicionado explícitamente en el debate de la Net neutrality.

- **Proveedores de acceso a Internet**

El debate sobre la Net neutrality presenta dos vertientes de negocio – no mutuamente excluyentes – para las empresas proveedoras de acceso a Internet, como Cisco, Ellacoya Networks o Lucent.

- **Usuarios**

La Consumer Federation of America, la Consumers Union, el US Public Interest Research Group y otras asociaciones para la defensa de los derechos de los usuarios de Internet están luchando en la actualidad para preservar el carácter libre y abierto que tradicionalmente ha distinguido a Internet.

- **Entidades reguladoras**

El regulador estadounidense ha defendido la Net neutrality a través de la definición de Internet como el derecho de los consumidores a una cuádruple libertad (contenidos, aplicaciones, conexión e información), pero hasta la fecha, ha sido reacio a formalizarla normativamente.

9.2.3 ***Argumentos de cada postura***

- **Proveedores de contenidos y/o servicios**

  - Innovación en las aplicaciones de Internet

    En Internet la inteligencia se encuentra en las aplicaciones (periferia) y no en los routers (centro). Esto es lo que se denomina estructura end-to-end (e2e) o punto a punto.

    Esta estructura ha impulsado que la innovación en Internet haya venido principalmente de la "frontera" o "extremo" de la red a través de la competencia en las aplicaciones. Una consecuencia de este diseño es que los proveedores de acceso no pudieron controlar en su momento fácilmente la innovación en el nivel de las aplicaciones que tenían lugar sobre sus redes. De este modo, la innovación en éstas pudo venir de muchos que no tenían ninguna conexión real con los propietarios de la red básica. De hecho, si se consideran algunas de las más importantes innovaciones de la historia de Internet –desde el desarrollo de la World Wide web al primer servicio de mensajería instantánea de Chat– todas ellas se caracterizan por ser innovaciones completamente ajenas a los propietarios de la red.

    Por otro lado, los proveedores de contenidos/servicios defienden igualmente que, como ha ocurrido en el pasado, la estructura flexible y adaptable de Internet asegurará su perduración en el tiempo. En la actualidad cualquier nueva aplicación sólo precisa un requisito para sobrevivir: que utilice el protocolo IP y que sea aceptada por la Red ya que ésta, en su condición e2e es, por definición, neutral.

    Parece extraño, pues, plantearse que lo que para muchos ha sido la clave del éxito de Internet hoy sea una causa de cambio en su concepción para alimentar nuevos modelos de negocio que alteren positivamente la cadena de valor del sector de las TIC.

    Sin embargo, los proveedores de servicios y contenidos de Internet consideran que, tal y como ha ocurrido históricamente, un mínimo control en la red maximiza el rango de competidores que pueden innovar para la red. La competencia se ampara en el diseño de la red y ha producido crecimiento.

    De este modo, estas empresas consideran que las pretensiones de las operadoras de telecomunicaciones acabarían por cambiar la esencia de Internet, que pasaría de ser potenciada por los usuarios (user-powered) a controlada por los operadores (carrier-controlled), lo que pondría en riesgo la eficacia que ha demostrado hasta ahora.

    En resumen, los proveedores de contenidos/servicios son partidarios de la evolución natural de la red basada en la tecnología como elemento clave para asegurar el futuro de Internet como espacio público de creatividad e innovación.

  - Inversiones. Modelo de negocio

    Los proveedores de contenidos/servicios son partidarios de que los operadores de red no les cobren nada y que el cobro se realice a los clientes mediante tarifas planas.

  - Libre competencia

    Los proveedores de contenidos/servicios consideran que es necesaria una legislación que ampare la Net neutrality para evitar prácticas como el 'acceso por escalones', que permitan a los

propietarios de la red condicionar el contenido o el derecho de los proveedores de acceso de proporcionar contenido o servicio sobre la red al pago de una contraprestación.

Sin embargo, a pesar de que este posicionamiento es común a todas las empresas proveedoras de contenidos, no todas ellas consideran el mismo grado de peligrosidad ante un posible control central de la red. Así, aunque todas ellas temen que los operadores de red abusen del control que tienen sobre las infraestructuras y utilicen su posicionamiento en el mercado para priorizar sus propios servicios por encima de los de los otros competidores, sólo algunas como Google y Vonage creen que los operadores de red van a bloquear completamente el tráfico, mientras que otras menos pesimistas consideran que los operadores de red únicamente van a limitar el ancho de banda de sus competidores para degradar el servicio ofrecido por sus competidores.

Por otro lado, algunos de los partidarios de la Net neutrality consideran que el "acceso-escalonado" favorecería a aquellas empresas mejor posicionadas (como Google) en detrimento de aquellas empresas incipientes. Las empresas ya consolidadas durante la época de desarrollo de Internet dispondrían de capacidad para asegurarse suficiente banda ancha para sus servicios y podrían dejar insuficiente capacidad a sus competidores. El 'acceso- escalonado' se convertiría así en una barrera de entrada difícil de salvar, y reduciría la competencia en aplicaciones y contenidos en Internet.

Los defensores de la Net neutrality consideran que añadir "peajes" a Internet puede beneficiar a los dueños de las "autopistas de la información" pero no beneficiará la competencia de aplicaciones y contenido en Internet, que impulsan el crecimiento económico.

No obstante, es necesario aclarar que en general los proveedores de contenidos/ servicios no son contrarios a todo tipo de "escalonamiento", sino que lo consideran una valiosa herramienta diferenciadora del servicio a nivel del usuario final que crearía (y efectivamente, crea) incentivos para que los proveedores de acceso mejoren la eficiencia de sus redes. Según los defensores de la Net neutrality, el escalonamiento en el nivel del consumidor no crearía ninguno de los efectos anticompetitivos que asumiría el "acceso-escalonado". En la medida en que los proveedores de acceso ofrezcan escalonamiento neutral, por ejemplo, ofreciendo alta velocidad para contenido de vídeo o simplemente mayor velocidad para transferencias de ficheros voluminosos, esta "discriminación" no dañará la competencia en el mercado de las aplicaciones. La diversidad de la demanda de los consumidores produciría una demanda general para un servicio de Internet más rápido y más barato. Este elemento beneficiaría también de forma general a la competencia en el mercado de aplicaciones.

- **Operadores de telecomunicaciones**

  - Seguridad y calidad frente a innovación

Las operadoras de telecomunicaciones afirman que la introducción del principio de Net neutrality como norma reguladora ex-ante, en un contexto cada vez más inclinado hacía una regulación ex-post, sería mucho peor que la eventual disminución de capacidad innovadora que argumentan los defensores de la neutralidad en caso de no legislar.

Una regulación ex-ante no permite priorizar entre contenidos: los paquetes de información circulan libremente por la estructura de Internet, que los direcciona de forma ciega, sin atender a sus contenidos. Los proveedores de servicios de banda ancha defienden que la aplicación de control centralizado permitiría dar respuesta a dos necesidades claras del mercado actual: seguridad y calidad.

Seguridad frente a conductas no amistosas

El vertiginoso paso de un uso exclusivo de Internet por parte de comunidades reducidas y homogéneas a millones de usuarios con intereses muy heterogéneos ha favorecido la proliferación de conductas no amistosas (hackers, fraudes,…), que han reducido exponencialmente la fiabilidad de la red. Debido a esto, se ha hecho evidente la necesidad de establecer algún tipo de control que evite/minimice los daños potenciales de determinadas conductas y contenidos.

Sin embargo, tal eventualidad se enfrenta con un grave problema: Internet apenas tiene establecidos en la actualidad mecanismos de seguridad en su arquitectura, y los que existen no permiten dar una respuesta global a esta necesidad.

Calidad de las nuevas aplicaciones

El desarrollo de Internet y el avance de las tecnologías, especialmente las relacionadas con la banda ancha, está haciendo posibles las aplicaciones intensivas en media streaming, fundamentalmente vídeo, que para su efectiva comercialización requieren unos determinados niveles de calidad. En concreto, se trata de evitar lo que en términos técnicos se conoce como latencias o retrasos en recepción de la imagen, que son resultado de que la arquitectura neutral de Internet no discrimine entre aplicaciones, colocando en un mismo nivel de prioridad una de estas aplicaciones de vídeo y un simple correo electrónico. Los proveedores de servicios consideran necesario establecer en Internet una cierta funcionalidad QoS (Quality Of Service) que permita discriminar entre distintas aplicaciones.

- Inversiones. Modelo de negocio

Las operadoras de telecomunicaciones consideran que tan importante como la innovación a nivel de aplicaciones en la periferia de la Red es la que se produce en su centro. Y es que tanto la disponibilidad como la capacidad de banda ancha son aspectos críticos para el desarrollo de la Sociedad de la Información y, por lo tanto, factor clave para la competitividad de las economías.

Las exigencias del desarrollo de la banda ancha a alta velocidad imponen a los operadores de telecomunicaciones la necesidad de continuar un proceso de inversión de dimensiones importantes y rentabilidades adecuadas a esas inversiones si no se preserva la capacidad de obtener réditos por su utilización.

Consideran que la única manera de incentivar la inversión de las operadoras de red, será la privatización en cierta medida de las redes. Argumentan que la legislación que impusiese la Net neutrality reduciría los incentivos para continuar invirtiendo en la actualización y en las mejoras de la infraestructura de la banda ancha. Además, impediría que aprovechasen la oportunidad de obtener ingresos adicionales para recuperar las inversiones ya realizadas que podrían ser reinvertidas en

mejoras y actualizaciones de las infraestructuras.

De este modo, el modelo de negocio planteado por las empresas que actualmente invierten en infraestructuras sería el de compartir tales inversiones al cobrar a los proveedores de servicios y contenidos en función del rendimiento: por ejemplo, Google pagaría a su proveedor de banda ancha una tasa para asegurarse que su página de búsqueda encuentra y muestra los resultados más rápidamente que las de sus competidores.

Un elemento a tener en cuenta de este modelo de negocio es el planteamiento de la idoneidad de esta regulación al tipo de fuerzas de mercado que afronta un proveedor de acceso y banda ancha. Este proveedor se enfrenta a un mercado con dos caras, puesto que existe una relación e interacción entre sus clientes y los proveedores de contenidos. Para que su negocio tenga éxito, necesita disponer de suficientes contenidos para atraer clientes y, simultáneamente, precisa suficientes clientes para atraer contenidos.

- Competencia

Dado que hasta el momento la actitud de los operadores no ha supuesto ningún riesgo para la libre competencia en el mercado (y en determinadas excepciones, el regulador ha actuado con prontitud), legislar la neutralidad en la red supondría crear una solución para un problema que no se ha planteado.

- **Operadores de cable**

No se han posicionado explícitamente en el debate de la Net neutrality. Sin embargo, de forma inherente a su negocio se oponen a la neutralidad de la Red puesto que la posibilidad de ofrecer "acceso escalonado" y servicios con posibilidad de priorizar suponen nuevas oportunidades de negocio igualmente fructíferas que para los operadores de telecomunicaciones.

- **Proveedores de acceso a Internet**

Por un lado, una red abierta con capacidad para albergar sin distinción a todos los servicios, aplicaciones y equipos servirá de motor de la innovación y favorecerá el crecimiento de la industria tecnológica. Si los operadores de telecomunicaciones estableciesen restricciones a las nuevas tecnologías como puede ser la Voz sobre IP sin impunidad, se generaría incertidumbre acerca de la viabilidad de cualquier tecnología emergente y esto impactaría negativamente en el crecimiento del sector de las TIC.

Por otro lado, las nuevas tecnologías de gestión de la red, desarrolladas por las empresas proveedoras de acceso, podrían ser utilizadas por los operadores de telecomunicaciones para ofrecer servicios de priorización y/o mejorar la calidad de sus servicios. Si se impusiese la Net neutrality como principio legislado, es posible que se frenase la necesidad de los operadores de telecomunicaciones de disponer de aplicaciones para una gestión priorizada y se inhibiría este mercado con gran potencialidad para las empresas suministradoras de acceso.

Así, los proveedores de acceso a Internet tienen intereses dobles (aunque no enfrentados) en el debate de la neutralidad de la Red. Consideran que debe mantenerse la posibilidad de que los usuarios finales puedan acceder a los contenidos y aplicaciones que deseen libremente, y que los operadores de red no debieran bloquear o degenerar el acceso del consumidor. Sin embargo, estas empresas consideran que los

operadores de red deberían gozar del derecho a administrar las características de la red, tanto para gestionar el tráfico, como para asegurar determinados niveles de calidad u ofrecer servicios escalonados. Y también consideran lógico que cobren cuotas por estos servicios y funcionalidades adicionales, siempre que se pruebe que éstos no hayan sido ofrecidos bajo criterios competitivos.

En resumen, consideran que el desarrollo de la industria tecnológica se mueve por la innovación. Y esta innovación tiene dos fuentes: la libertad de experimentar en la red, que hace que el proceso de creación y análisis de viabilidad de las nuevas tecnologías se acelere (visión compartida con los proveedores de contenidos y servicios); y por las necesidades de nuevas aplicaciones y herramientas para controlar la calidad del servicio de la red y priorizar (visión compartida con los operadores de red).

- **Usuarios**

Asociaciones en defensa de los derechos humanos argumentan que un modelo no neutral de la Red probablemente acabará obligando a los consumidores a pagar su acceso a Internet por partida doble: pagarán primero por el acceso en sí mismo, y después, por los contenidos y servicios que utilicen.

- **Entidades reguladoras**

La Corte Suprema de los Estados Unidos sostiene, a favor de los operadores de red, que ninguna práctica empresarial debería ser prohibida de antemano, ya que sólo éstas deberían serlo en caso que se logre demostrar su efecto anticompetitivo. Al mismo tiempo, considera que la Net neutrality podría reducir potencialmente los incentivos que tienen los operadores para la construcción de nuevas redes (o la ampliación de las existentes).

La Federal Communications Comission (FCC) está manteniendo una posición objetiva y prudente del tratamiento de la Net neutrality. Por un lado, parece estar defendiendo la neutralidad, y consecuentemente a las empresas de Internet, aunque no su instauración como principio regulatorio. Sólo refuerza la idea de una Internet libre que conserve una Net neutrality de facto en beneficio de los usuarios finales, a quienes debe garantizárseles el acceso a la información y el uso de aplicaciones. La FCC confía plenamente en las fuerzas del mercado, y no advierte la necesidad de generar una normativa que formalice la Net neutrality. Sin embargo, en una actitud preventiva, instó a los operadores de red a desistir de cualquier acción de bloqueo para el tráfico correspondiente a servicios de Internet que se canalice a través de sus redes de acceso. En este sentido, el regulador se alinea con los operadores que defienden la libertad de mercado y la competencia entre tecnologías de acceso como la mejor protección de la Red.

Ambas posiciones se encuentran enfrentadas en cuanto a la forma pero no en cuanto al fondo, es decir, ambas buscan el mejor progreso de Internet, en cuanto a innovación, la inversión y el desarrollo de servicios, aplicaciones, contenidos, usuarios, etc. pero divergen en cuanto al medio óptimo para alcanzar estos fines.

CAPÍTULO 10: TENDENCIAS EN AUDITORÍA Y SEGUIRDAD INFORMÁTICA

10. TENDENCIAS EN AUDITORÍA Y SEGURIDAD INFORMÁTICA

10.1 EL RIESGO DE PREDECIR LO QUE PASARÁ

Siempre es un reto y un riesgo tratar de hacer predicciones y más en seguridad de la información, mejor en inseguridad de la información. Conforme la inseguridad avanza, nuevas estrategias de protección se generan, lo cual nos muestra que la industria de seguridad, en términos tecnológicos, es una de las más activas en el mundo. Bien, en este sentido trataremos de hacer una visión hacia delante sobre las variaciones y efectos de la inseguridad informática considerando los actuales móviles de las actividades que se han manifestado y prometen seguir.

10.1.1. Evoluciona la "ciberguerra fría"

El tema de protección de infraestructura crítica estará a la orden de día, pues se advierten ya muchas formas de penetrar los escudos y defensas de las naciones industrializadas, las cuales ven en esta tendencia una amenaza real y tangible, algo que no puede pasar de desapercibido y requiere recursos y atención especializada. Si en el pasado la guerra fría era la amenaza nuclear, ahora la amenaza se establece en ataques masivos y toma de control de principales sistemas de misión crítica de un estado como son: la banca central, el sistema bancario, los servicios públicos, los hospitales y servicios de emergencia, gasoductos y poliductos, entre otros.

10.1.2. Se transforma la inseguridad en las aplicaciones

La rápida apropiación del web y las posibilidades de tener mayores servicios e interacción, abre nuevas relaciones que aún no conocemos con claridad y que serán objeto de análisis y revisión tanto por analistas de seguridad como por los intrusos. El paso de las aplicaciones orientada al WEB, basada en interacción sobre el protocolo http a una donde los mensajes que viajan son XML, establecen un nuevo paradigma en las aplicaciones denominado Web Services. La promesa de estas nuevas tecnologías es tener acceso a los servicios en cualquier momento, en cualquier lugar, sin preocuparse por la implementación del mismo, sólo utilizarlo o como dirían los programadores, consumirlo. En este nuevo contexto, los riesgos de seguridad cambian y ahora ya las medidas de seguridad heredadas del mundo web y del mundo cliente/servidor no son aplicables en toda su dimensión, con lo cual sugiere repensar nuevamente la inseguridad informática por parte de los programadores.

10.1. 3. Se acentúa la amenaza de incidente de seguridad interno

El factor humano es y será parte de ese eslabón débil de la cadena de la seguridad. Una cadena que tiene tantas debilidades o inseguridades como las personas mismas. Pero igualmente tantas oportunidades y desafíos como las inquietudes y creaciones de las personas que hacen parte de la organización. Esta paradoja de la seguridad informática, plantea un escenario de múltiples variables y componentes que deben ser parte de la agenda del estratega de la seguridad de la información. Las personas son la fuente de las amenazas y de los controles, luego un estudio juicioso de esta realidad es necesario, no para resolver esta variable en la ecuación de la seguridad, sino para repensarla y explorar nuevas posibilidades de control, entendiendo este concepto, como la capacidad de orientación para llevar el sistema a un mejor funcionamiento.

10.1.4. Las iniciativas normativas y regulatorias se hacen más evidentes

Las noticias tanto nacionales como internacionales sobre exposición de datos, fugas de información, transacciones electrónicas fraudulentas, robos de identidades entre otras, ha alertado a las organizaciones gubernamentales sobre la realidad de la inseguridad de la información y los impactos de ésta en la competitividad de las naciones.

10.1.5. Muchos estándares, muchos procedimientos, poco gobierno y poca interiorización en seguridad de la información

Hemos experimentado durante los últimos años una explosión de estándares, buenas prácticas y recomendaciones sobre la seguridad de la información que buscan ofrecer a las organizaciones lineamientos para organizar y administrar este tema. El resultado de la aplicación de los mismos ha llevado a mejorar la formalización de la práctica de seguridad en términos operacionales y tácticos, algo que, si bien es positivo, nos ha rezagado en la madurez de la función de seguridad informática. Este rezago se debe que estamos trabajando en el fortalecimiento de la credibilidad y funcionalidad de los procesos de seguridad informática, pero no se avanza formalmente en la proyección e interiorización de los mismos en las instancias de gobierno. La seguridad de la información se percibe como "algo que otros piensan por mí" y no como algo de lo cual "yo soy responsable" como "primer custodio de la información". En este escenario se plantea una paradoja interesante, por un lado querer cumplir con la regulación que sobre el tema se manifieste y por otro, "creerme" que el tema es importante, no sólo por las sanciones que me pueden llegar si incumplo la norma, sino como elemento estratégico para darle mayor valor a los clientes y al negocio, es decir, dejar de asumirlo como gasto y entenderlo como inversión.

10.2 TENDENCIAS EN AUDITORÍA INFORMÁTICA

La entrada en vigor, durante 2006, de la norma ISO/IEC 27001 como estándar mundial para los Sistemas de Gestión de Seguridad de la Información SGSI y sus requerimientos de Auditoría para la obtención de las certificaciones, también han supuesto un gran incremento de la demanda de Auditores Informáticos. Otros estándares en los que ya está participando España, como los Criterios Comunes, también precisan de Auditores de Seguridad de Productos y Sistemas Informáticos.

En España la LOPD (Ley Orgánica de Protección de Datos Personales) está sirviendo de base para que en nuestro país el Auditor en Informática sea un profesional cada vez más solicitado. En la actualidad tanto en las Empresas Privadas como en las Administraciones y Organismos Públicos se están llevando a cabo proyectos de adecuación de sus Sistemas Informáticos a la LOPD que requieren de la Auditoría Informática.

Aunque en la actualidad la legislación existente relacionada con la Informática sigue siendo escasa, en los últimos años los Gobiernos comienzan a tomar conciencia de la necesidad de exigir responsabilidades en los riesgos derivados de los sistemas informáticos y de la necesidad de establecer controles adecuados. Podemos observar cómo en estas nuevas leyes la Auditoría Informática siempre está presente.

La Auditoría y Seguridad Informática avanzan en paralelo en la nueva Sociedad de la Información, que con su propio afianzamiento está incrementando la demanda de Auditores en Informática e Ingenieros especializados en Seguridad Informática.

10.3 TENDENCIAS EN SEGURIDAD INFORMÁTICA

La visión de las tendencias en seguridad informática según Symantec es:

- **Evolución de bots**: Esperan que los bots evolucionen y se diversifiquen en su manera de operar. Quizás, por ejemplo, podríamos llegar a ver situaciones como sitios de phishing hospedados por ordenadores con bots.
- **Amenazas avanzadas de Web**: A medida que el número de servicios Web aumenta y los navegadores interpretan de manera uniforme del lenguaje de códigos como Java Script, Symantec espera que el número de amenazas basadas en Web se incremente.
- **Plataformas móviles**: El interés en seguridad móvil está en su punto más alto. A medida que los teléfonos se vuelven más complejos, más interesantes y más conectados, se espera que los atacantes tomen ventaja de ello.
- **Evolución del Spam**: Symantec espera ver que el spam continúe evolucionando para evadir los sistemas tradicionales de bloqueo y hacer que los usuarios abran los correos no deseados.
- **Mundos virtuales**: Symantec espera que mientras continúe aumentando el uso de mundos virtuales y los juegos en línea que involucran a múltiples jugadores se hagan más populares, surgirán nuevas amenazas ya que los criminales, phishers, spammers y otros delincuentes digitales pondrán su atención en estas nuevas comunidades.
- **Campañas electorales**: Especialmente en Estados Unidos, a medida que los candidatos políticos utilicen Internet como parte de sus campañas no deben perder de vista que existen diversos riesgos de seguridad asociados a las TI. Estos riesgos incluyen, entre otros, la difusión de donaciones en línea para las campañas; el envío de información errónea; fraude; phishing; y la invasión de la privacidad.

10.4 ¿QUÉ NOS DEPARA EL MALWARE EN EL FUTURO?

El malware sigue llevando adelante sus acciones dañinas, ampliando sus frentes de ataque y mejorando su efectividad.

Es así que en la actualidad, la variedad de los tipos de malware, como así también las dimensiones que abarcan sus efectos, han ido en aumento destacándose ciertas cuestiones que hacen de este tipo de programas, las amenazas más importantes y más difíciles de combatir en cualquier entorno informático.

- Abuso de confianza del usuario

  La Ingeniería Social sigue siendo el elemento más explotado para engañar e infectar al usuario. Esto queda demostrado con la aparición de gran cantidad de malware que utilizan las tarjetas virtuales y los eventos de gran envergadura para incitar al usuario a que descargue un archivo dañino.

  La formación de grandes comunidades online (como MySpace, Orkut, FaceBook y diferentes juegos en línea) también se ha convertido en un importante punto para abusar de la confianza de los usuarios. Actualmente, ya existe gran cantidad de malware disponible para robar los datos privados a los usuarios que participan de estas comunidades.

  También es válido lo mencionado anteriormente para los ataques de phishing, cuyos anzuelos se perfeccionan y se hacen más eficaces. Técnicas

antiguas, como por ejemplo pharming local, siguen siendo utilizadas masivamente y los principales bancos latinoamericanos (y sus usuarios) se están convirtiendo en el epicentro de estos ataques, a través de correos masivos y troyanos.

Un ejemplo de perfeccionamiento de estas técnicas son los casos en donde los ataques de phishing no implican la clonación de páginas web para robar información sensible de los usuarios sino que, contrariamente a ello, utilizan metodologías mediante las cuales superponen, en la zona de acceso al Home-Banking, una imagen similar a la real.

- Abuso de recursos de Internet

Teniendo en cuenta este escenario, hoy se continúa siendo testigo de que la natural evolución del malware seguirá en aumento y seguirá perfeccionándose con técnicas y metodologías de todo tipo pudiendo alcanzar niveles preocupantes.

Con relación al correo electrónico no deseado y no solicitado (comúnmente denominado spam) se percibe un gran avance en las metodologías de engaño que utilizan los creadores de malware para acaparar la atención de los usuarios; por ejemplo la masificación de mensajes conteniendo imágenes y el nacimiento del spam en archivos PDF y MP3.

El robo de inmensas bases de datos de diferentes organizaciones mundiales permite ataques dirigidos a usuarios a través de spam y de phishing personalizado. Por esto, se volverá más común encontrar que el spam sea dirigido a una persona con nombre y apellido, e incluso en el idioma nativo del propietario de las cuentas de correo.

Por otro lado, aprovechando las nuevas tecnologías de comunicación de las comunidades online ya mencionadas, el spam común y corriente se está trasladando a estas comunidades en formato de splog (comentarios en blogs enlazando a sitios dañinos).

La aparición de servicios gratuitos tipo mash-up, en donde un sitio web no vulnerable "recibe" servicios de otros que pueden ser vulnerables, se está afianzando y cada vez es más normal encontrar enlaces a sitios conocidos que contienen servicios de terceros que apuntan a código dañino. Esto incluso sucede en cualquier buscador y con cualquier tema de referencia.

- Vulnerabilidades

Un apartado especial se merece los errores que todo software tiene como común denominador. La explotación de vulnerabilidades a través de los navegadores es una de las técnicas que más se ha perfeccionado y día a día surgen nuevos exploits y nuevos scripts (generalmente ofuscados para evadir a las herramientas de seguridad) que aprovechan determinadas debilidades en los sitios web comprometidos y que permiten la instalación de malware en los equipos de los usuarios.

Debe remarcarse que la tendencia actual de los creadores de malware es infectar a una gran cantidad de usuarios en forma totalmente silenciosa a través de códigos ocultos en sitios web, para pasar desapercibidos. Sin duda, esta técnica resulta más eficiente que un ataque masivo y rápido que alerta a los usuarios y a las compañías de seguridad.

- Nuevas tecnologías

El aprovechamiento de las nuevas tecnologías sigue creciendo al igual que sus vulnerabilidades y formas de explotación. En este sentido, tecnologías como voz sobre IP no fueron la excepción y también terminaron siendo explotadas por el malware.

Asimismo, se debe hacer referencia a la creación de programas dañinos para productos de reciente aparición como nuevas versiones del iPod y el iPhone. Si bien las infecciones no han sido masivas, son las suficientes como para marcar el camino en este aspecto.

Por otro lado, la utilización de clientes de mensajería instantánea y las redes P2P para propagar malware son moneda corriente.

La diseminación y posterior infección por intermedio de dispositivos de almacenamiento extraíbles (USB, memorias, flash, etc.) que aprovechan las bondades de ejecución automáticas de los sistemas operativos, se ha ido acrecentando y todo indica que seguirá creciendo aún más.

- Las amenazas de siempre potenciadas

Troyanos, gusanos y PUP (Potencial Unwanted Programs; o en castellano programas potencialmente no deseados) son cada vez más sofisticados a punto tal que incorporan capacidades defensivas que hacen que la tarea de análisis y remoción sea más complicada. Por ejemplo, muchos de ellos ya cuentan con la habilidad de detectar cuando son ejecutados en máquinas virtuales o cuando están siendo analizados.

- Conclusiones

Se debe remarcar la gran actuación que tuvieron y tienen las redes organizadas para el crimen en todo este panorama: la interoperación de spammers, phishers, botmasters y creadores de malware hacen que a veces Internet se convierta en un lugar agresivo transformando a los usuarios en mulas (aquellos que mueven dinero sin saberlo y generalmente previamente engañados).

Además, hay un factor que permanece intacto y permanecerá así por mucho tiempo más, sin importar el tipo de amenaza que se trate ni las diferentes metodologías que utilice, un componente fundamental que ningún código malicioso desperdicia ni deja de monopolizar: la Ingeniería Social.

Pero a pesar de la utilización de esta técnica, los usuarios deben ser conscientes de que cuentan con una herramienta mucho más sofisticada: la educación, que aplicada de forma oportuna, permite potenciar las posibilidades de no ser víctimas del malware en general o de cualquier amenaza que a nivel informático se presente.

CONCLUSIONES GENERALES

CONCLUSIONES GENERALES

La elaboración de este proyecto ha supuesto un gran esfuerzo de trabajo y tiempo, ya que se ha tenido que investigar temas como calidad, seguridad y auditoría, así como diferentes estándares y métricas. Se ha tenido que ir actualizando la información, ya que se han ido publicando nuevas normas y estándares.

Además se ha incorporado una parte práctica, para aplicar conocimientos adquiridos durante el desarrollo, como es la ISO 20000.

La finalidad ha sido crear conciencia de calidad y seguridad a todas las personas implicadas en labores informáticas.

Con el fin de valorar el resultado, se estima oportuno recordar los objetivos que se plantearon cuando se elaboró el marco general del proyecto:

La calidad en el desarrollo y mantenimiento del software, así como la seguridad del mismo y de los equipos informáticos, se ha convertido hoy en día en uno de los principales objetivos estratégicos de las organizaciones, debido a que cada vez más, los procesos principales de las organizaciones (y su supervivencia) dependen de los sistemas informáticos para su buen funcionamiento.

La calidad es la base de la productividad, y ésta es el auténtico motor del desarrollo económico, algo que está por encima del mero crecimiento económico.

En la evolución experimentada por la calidad del software se ha pasado de un tratamiento centrado fundamentalmente en la inspección y detección de errores, a una aproximación más sistemática, dada la importancia que ha adquirido la calidad en la ingeniería del software.

En los últimos años se han publicado diversos estudios y estándares en los que se exponen los principios que se deben seguir para la mejora tanto de productos como de procesos software. Todo ello ha influido de forma significativa en el papel que actualmente tiene la calidad en las organizaciones, que pasa a convertirse en una filosofía y una cultura que afecta a toda la organización.

La seguridad informática se ha vuelto cada día más compleja para las empresas. Cada año se contabilizan pérdidas millonarias en las empresas debido a los numerosos ataques de virus y violaciones a la seguridad informática.

Hoy en día las empresas deben enfocar parte de su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las cuentan para hacerle frente a los posibles ataques informáticos que luego se puedan traducir en pérdidas cuantiosas de dinero.

La seguridad forma parte de la organización y ha de gestionarse de forma continuada, desde el momento de la creación de la información hasta el momento de su destrucción.

En la actualidad es de vital importancia el considerar realizar auditorías informáticas, que aseguren que se están cumpliendo los objetivos establecidos.

Teniendo en cuenta estos puntos, se puede observar, que cada persona que lea este proyecto, comprenderá la importancia de dichos puntos, que era la pretensión que se tenía a la hora de desarrollar este proyecto.

Sin duda, el campo de la mejora y evaluación de procesos es muy prolífico y emergente, un campo muy activo de trabajo. Por este motivo, siempre se tendría que estar actualizando la información presentada en este proyecto, ya que los mismos estándares van evolucionando y cambiando.

Quedan importantes temas abiertos, como el acercamiento de estos estándares e ISOS a las empresas.

Así también, se podría profundizar más en estos temas, dedicando un proyecto para cada tema tratado, como para cada norma.

En líneas futuras, se podrían estudiar otras ISOS no especificadas en este proyecto, como por ejemplo la ISO 9001 referente a la calidad, o las ISOS especificadas en el apéndice de ISOS, que si bien no todas se refieren a calidad y seguridad o auditoría informática, la aplicación de las mismas asegurará que se tengan unos buenos resultados.

Además se podría desarrollar una aplicación que no sólo estimara el buen funcionamiento en una empresa de la ISO 20000, sino el conjunto de varias normas, teniendo en cuenta el flujo de la información, los soportes informáticos, así como el personal implicado.

Queda a disposición del lector, el poder profundizar en estas propuestas, para una mayor comprensión de los temas.

APÉNDICE A: LISTAS DE NORMAS ISO

LISTA DE NORMAS ISO

Normas ISO: 1-999/Idiomas y caracteres

- ISO 16: Afinación en LA 440 Hz.
- ISO 216: Medidas de papel: p.e. ISO A4.
- ISO 639: Nombres de lenguas.
- ISO 690: 1987 regula las citas bibliográficas (corresponde a la norma UNE 50104:1994).
- ISO 690-2: 1997 regula las citas bibliográficas de documentos electrónicos.
- ISO 732: Formato de carrete de 120.
- ISO 838: Estándar para perforadoras de papel.

Normas ISO: 1000-8999/Sistema Internacional de Medidas, Códigos y lenguajes

- ISO 1007: Formato de carrete de 135.
- ISO/IEC 1539-1: Lenguaje de programación Fortran.
- ISO 2789: Información y documentación: estadísticas internacionales de bibliotecas.
- ISO 3029: Formato carrete de 126.
- ISO 3166: Códigos de países.
- ISO 4217: Códigos de divisas.
- ISO 7811: Técnica de grabación en tarjetas de identificación.
- ISO 8601: Representación del tiempo y la fecha. Adoptado en Internet mediante el Date and Time Formats de W3C que utiliza UTC.
- ISO 8859: codificaciones de caracteres que incluye ASCII como un subconjunto (Uno de ellos es el ISO 8859-1 que permite codificar las lenguas originales de Europa occidental, como el español).
- ISO/IEC 8652: 1995 Lenguaje de programación Ada.

Normas ISO: 9000-9099/Calidad

- ISO 9000: Sistemas de Gestión de la Calidad.
- ISO 9000: Sistemas de Gestión de la Calidad - Fundamentos y vocabulario.
- SO 9001: Sistemas de Gestión de la Calidad – Requisitos.
- ISO 9004: Sistemas de Gestión de la Calidad - Directrices para la mejora del desempeño.
- ISO 10011: Sistemas de Gestión de la Calidad - Directrices para auditorías.
- [ISO 19011]: Sistema de Gestión de Calidad - Auditoría de Calidad.
- ISO 8402: Sistemas de Gestión de la Calidad - Gestión de la calidad.
- ISO 10011: Sistemas de Gestión de la Calidad.

Normas ISO: 9100-9999/Programas, códigos y lenguajes informáticos

- ISO 9660: Sistema de archivos de CD-ROM.
- ISO 9899: Lenguaje de programación C.

- ISO/IEC 90003: Ingeniería del Software.

Normas ISO: 10000-13999

- ISO 10279: Lenguaje de programación BASIC.
- ISO 10646: Universal Carácter Set.
- ISO/IEC 11172: MPEG-1.
- ISO/IEC_12207: Tecnología de la información / Ciclo de vida del software.
- ISO13450: Formato de carrete de 110.
- ISO/IEC 13818: MPEG-2.

Normas ISO: 14000/Medioambiente

- ISO 14000: Estándares de Gestión Medioambiental en entornos de producción.

Normas ISO: 14400-15999

- ISO/IEC 14496 MPEG-4.
- ISO/IEC 15444 JPEG 2000.
- ISO/IEC 14443: Estándar para tarjetas inteligentes de proximidad.
- ISO 15693: Estándar para "tarjetas de vecindad".

Normas ISO/TS 16949

La especificación ISO TS 16949 es una ampliación de la serie de normas internacionales ISO 9000 para la industria del automóvil, con requisitos específicos del sector y del cliente. Es el resultado de una armonización de las normas:

- QS 9000: de origen estadounidense (con Chrysler, Ford y General Motors)
- VDA 6.1 de origen alemán.
- EAQF de origen francés.
- AVSQ de origen italiano.

Normas ISO: 19200-20000

Normas ISO: 22000/Sistema de gestión de la seguridad de los productos alimentarios

Normas ISO: 26000/Responsabilidad social de las organizaciones

- ISO 26000.

Normas ISO: 27000/ Seguridad de la información

- ISO/IEC 27001 y 27002: Sistema de Gestión de Seguridad de la Información.

APÉNDICE B: ISO 27000

APÉNDICE A: ISO 27000

INTRODUCCIÓN

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados (o en fase de desarrollo) por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumirán las distintas normas que componen la serie ISO 27000 y se indicará cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

ORIGEN

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

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

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

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

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

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

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

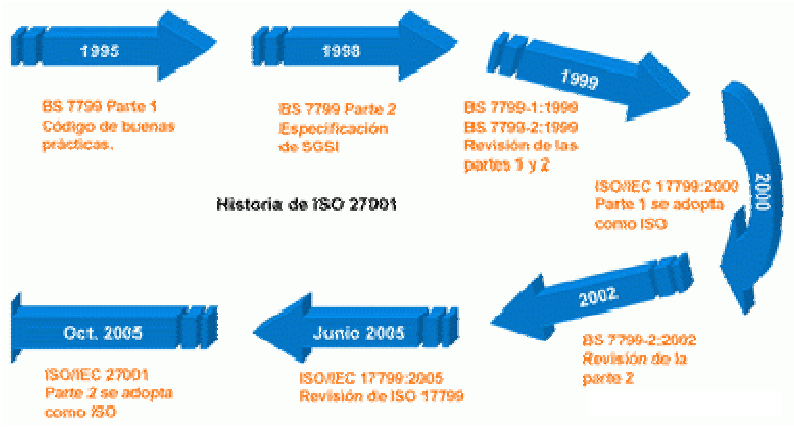


Imagen 8: Historia ISO 27001

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

LA SERIE 27000

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

- **ISO 27000:** Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.
- **ISO 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007.
- **ISO 27002:** Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

- **ISO 27003:** Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- **ISO 27004:** Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.
- **ISO 27005:** Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.
- **ISO 27006:** Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.
- **ISO 27007:** Se encuentra en fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.
- **ISO 27011:** Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).
- **ISO 27031:** Se encuentra en fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- **ISO 27032:** Consiste en una guía relativa a la ciberseguridad.
- **ISO 27033:** Se encuentra en fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante *Gateway*, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028.

- **ISO 27034:** Consiste en una guía de seguridad en aplicaciones.
- **ISO 27799:** Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

CONTENIDO RESUMIDO

ISO 27001:2005

- **Introducción:** generalidades e introducción al método PDCA.
- **Objeto y campo de aplicación:** se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- **Normas para consulta:** otras normas que sirven de referencia.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- **Sistema de gestión de la seguridad de la información:** cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- **Responsabilidad de la dirección:** en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- **Auditorías internas del SGSI:** cómo realizar las auditorías internas de control y cumplimiento.
- **Revisión del SGSI por la dirección:** cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- **Mejora del SGSI:** mejora continua, acciones correctivas y acciones preventivas.
- **Objetivos de control y controles:** anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
- **Relación con los Principios de la OCDE:** anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.

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

ISO 27002:2005 (anterior ISO 17799:2005)

- **Introducción:** conceptos generales de seguridad de la información y SGSI.
- **Campo de aplicación:** se especifica el objetivo de la norma.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- **Estructura del estándar:** descripción de la estructura de la norma.
- **Evaluación y tratamiento del riesgo:** indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- **Política de seguridad:** documento de política de seguridad y su gestión.
- **Aspectos organizativos de la seguridad de la información:** organización interna; terceros.
- **Gestión de activos:** responsabilidad sobre los activos; clasificación de la información.
- **Seguridad ligada a los recursos humanos:** antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- **Seguridad física y ambiental:** áreas seguras; seguridad de los equipos.
- **Gestión de comunicaciones y operaciones:** responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- **Control de acceso:** requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- **Gestión de incidentes de seguridad de la información:** notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- **Cumplimiento:** cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

ISO 27005:2008

Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- **Preámbulo**
- **Introducción**
- **Referencias normativas**
- **Términos y definiciones**
- **Breve descripción de los términos más usados en la norma.**
- **Estructura del estándar**
- **Descripción de la estructura de la norma.**
- **Fundamentos del proceso de gestión de riesgos (ISRM)**
- **Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.**
- **Establecimiento del contexto**
- **Evaluación de riesgos (ISRA)**
- **Tratamiento de riesgos**
- **Aceptación del riesgo**
- **Comunicación del riesgo**
- **Monitorización y revisión del riesgo**
- **Anexo A: Definiendo el ámbito del proceso**
- **Anexo B: Valoración de activos y evaluación de impacto**
- **Anexo C: Ejemplos de amenazas más comunes**
- **Anexo D: Vulnerabilidades y métodos de evaluación**
- **Anexo E: Aproximación a ISRA**

ISO 27006:2007

(Esta norma referencia directamente a muchas cláusulas de ISO 17021, requisitos de entidades de auditoría y certificación de sistemas de gestión, por lo que es recomendable disponer también de dicha norma).

- **Preámbulo:** presentación de las organizaciones ISO e IEC y sus actividades.
- **Introducción:** antecedentes de ISO 27006 y guía de uso para la norma.
- **Campo de aplicación:** a quién aplica este estándar.
- **Referencias normativas:** otras normas que sirven de referencia.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.

- **Principios:** principios que rigen esta norma.
- **Requisitos generales:** aspectos generales que deben cumplir las entidades de certificación de SGSIs.
- **Requisitos estructurales:** estructura organizativa que deben tener las entidades de certificación de SGSIs.
- **Requisitos en cuanto a recursos:** competencias requeridas para el personal de dirección, administración y auditoría de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratas.
- **Requisitos de información:** información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.
- **Requisitos del proceso:** requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, recertificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.
- **Requisitos del sistema de gestión de entidades de certificación:** opciones, opción 1 (requisitos del sistema de gestión de acuerdo con ISO 9001) y opción 2 (requisitos del sistema de gestión general).
- **Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector:** potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.
- **Anexo B - Áreas de ejemplo de competencia del auditor:** consideraciones de competencia general y consideraciones de competencia específica (conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGSIs).
- **Anexo C - Tiempos de auditoría**: introducción, procedimiento para determinar la duración de la auditoría y tabla de tiempos de auditoría (incluyendo comparativa con tiempos de auditoría de sistemas de calidad -ISO 9001- y medioambientales -ISO 14001-).
- **Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005:** tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

ISO 27799:2008

Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma.

- **Alcance**
- **Referencias (Normativas)**
- **Terminología**

- **Simbología**
- **Seguridad de la información sanitaria** (Objetivos; Seguridad en el gobierno de la información; Información sanitaria a proteger; Amenazas y vulnerabilidades)
- **Plan de acción práctico para implantar ISO 17799/27002** (Taxonomía; Acuerdo de la dirección; establecimiento, operación, mantenimiento y mejora de un SGSI; Planning; Doing; Checking, Auditing)
- **Implicaciones sanitarias de ISO 17799/27002** (Política de seguridad de la información; Organización; gestión de activos; RRHH; Físicos; Comunicaciones; Accesos; Adquisición; Gestión de Incidentes; Continuidad de negocio; Cumplimiento legal)
- **Anexo A:** Amenazas
- **Anexo B:** Tareas y documentación de un SGSI
- **Anexo C:** Beneficios potenciales y atributos de herramientas
- **Anexo D:** Estándares relacionados

BENEFICIOS

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

¿CÓMO ADAPTARSE?

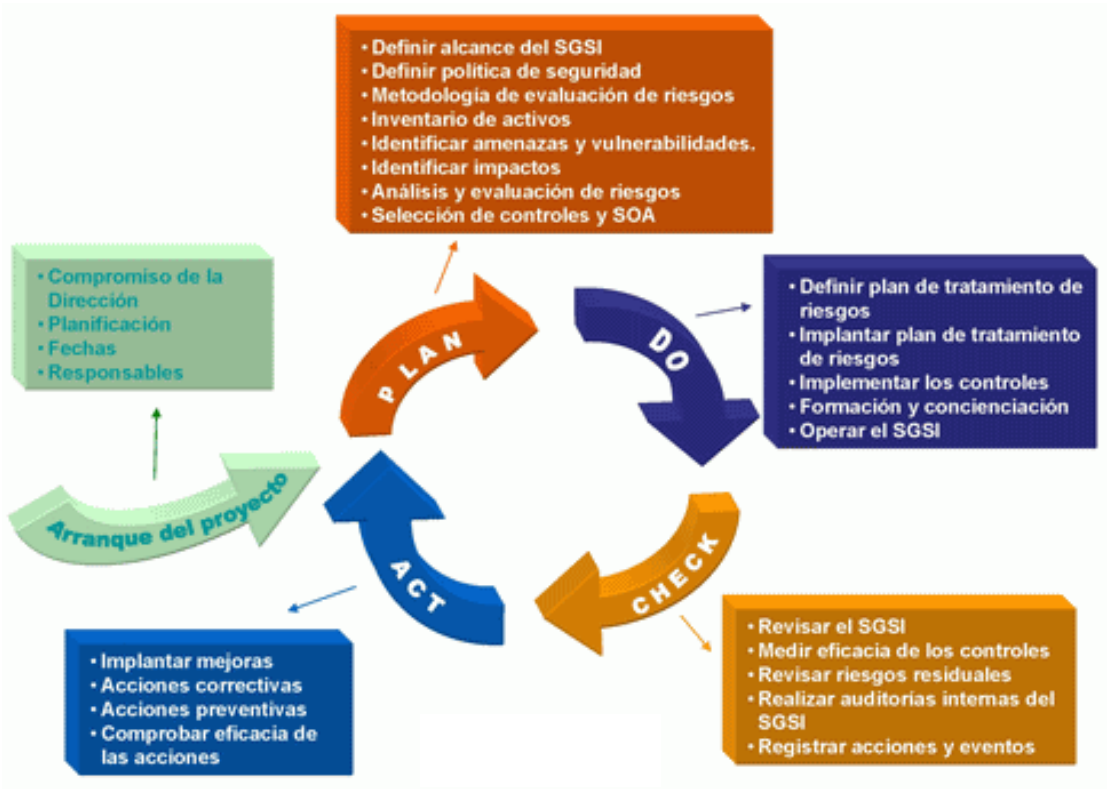


Imagen 9: ISO 27001 - ¿Cómo adaptarse?

Arranque del proyecto

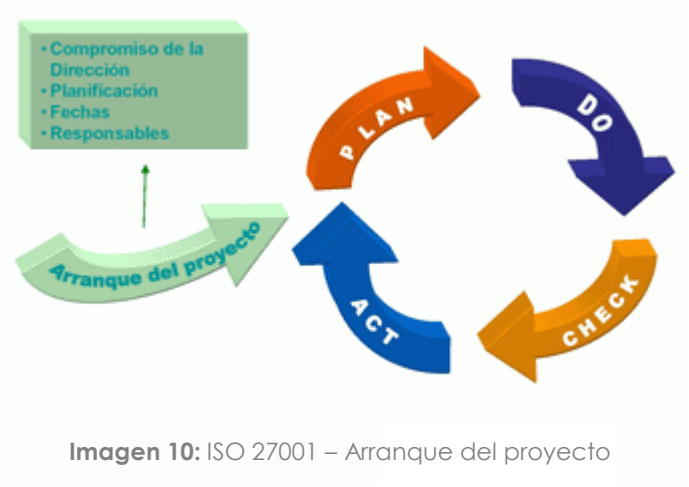


Imagen 10: ISO 27001 – Arranque del proyecto

- Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.

- Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

Planificación

Imagen 11: ISO 27001 – Planificación

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente (ver sección de Herramientas); la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Implementación

Imagen 12: ISO 27001 – Implementación

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Seguimiento

Imagen 13: ISO 27001 – Seguimiento

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Mejora continua

Imagen 14: ISO 27001 – Mejora Continua

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Aspectos Clave

Fundamentales

- Compromiso y apoyo de la Dirección de la organización.
- Definición clara de un alcance apropiado.

- Concienciación y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Integración del SGSI en la organización.

Factores de éxito

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

Riesgos

- Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

Consejos básicos

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
- Comprender en detalle el proceso de implantación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.
- Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.
- La autoridad y compromiso decidido de la Dirección de la empresa (incluso si al inicio el alcance se restringe a un alcance reducido) evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.
- La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.
- No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.
- Servirse de lo ya implementado: otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.
- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

APÉNDICE C: ISO 20000

ISO 20000

La serie ISO/IEC 20000 - Service Management normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotchnical Commission) el 14 de Diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización británica, The British Standars Institution (BSI).

ORGANIZACIÓN

El estándar se organiza en dos partes:

- Parte 1: ISO/IEC 20000-1:2005 - Especificación. Preparada por BSI como BS 15000-1
- Parte 2: ISO/IEC 20000-2:2005 - Código de Prácticas. Preparada por BSI como BS 15000-2

La primera parte (Especificación) define los requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio, con calidad y valor añadido para los clientes, asegurando una optimización de los costes y garantizando la seguridad de la entrega en todo momento. El cumplimiento de esta parte, garantiza además, que se está realizando un ciclo de mejora continuo en la gestión de servicios de TI. La especificación supone un completo sistema de gestión (organizado según ISO 9001) basado en procesos de gestión de servicio, políticas, objetivos y controles. El marco de procesos diseñado se organiza en base a los siguientes bloques:

- Grupo de procesos de Provisión del Servicio.
- Grupo de procesos de Control.
- Grupo de procesos de Entrega.
- Grupo de procesos de Resolución.
- Grupo de procesos de Relaciones.

Su alcance incluye:

- requisitos para un sistema de gestión
- planificación e implantación de la gestión del servicio
- planificación e implantación de servicios nuevos o cambiados
- proceso de prestación de servicios
- procesos de relaciones
- procesos de resolución
- procesos de control y liberación

La segunda parte (Código de Prácticas) representa el conjunto de buenas prácticas adoptadas y aceptadas por la industria en materia de Gestión de Servicio de TI. Está basada en el estándar de facto ITIL (Biblioteca de Infraestructura de TI) y sirve como guía y soporte en el establecimiento de acciones de mejora en el servicio o preparación de auditorías contra el estándar ISO/IEC 20000-1:2005.

CERTIFICACIÓN

La aparición de la serie ISO/IEC 20000, ha supuesto el primer sistema de gestión en servicio de TI certificable bajo norma reconocida a nivel mundial. Hasta ahora, las organizaciones podían optar por aplicar el conjunto de mejoras prácticas dictadas por ITIL (completadas por otros estándares como CMMI o CoBIT) o certificar su gestión contra el estándar local británico BS 15000. La parte 1 de la serie, ISO/IEC 20000-1:2005 representa el estándar certificable. En Febrero de 2006, AENOR (organización delegada en España de ISO/IEC) inició el mecanismo de adopción y conversión de la norma ISO/IEC 20000 a norma UNE. El viernes 23 de Junio de 2006, la organización itSMF hace entrega a AENOR de la versión traducida de la norma. En el BOE del 25 de julio de 2007 ambas partes se ratificaron como normas españolas con las siguientes referencias:

- UNE-ISO/IEC 20000-1:2007 Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones (ISO/IEC 20000-1:2005).
- UNE-ISO/IEC 20000-2:2007 Tecnología de la información. Gestión del servicio. Parte 2: Código de buenas prácticas (ISO 20000-2:2005).

Estas normas pueden adquirirse a través del portal web de AENOR. Cualquier entidad puede solicitar la certificación respecto a esas normas.

¿QUÉ ES ISO 20000?

La norma ISO 20000 se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia, los problemas se clasifican, lo que ayuda a identificar problemas continuados o interrelaciones. La norma considera también la capacidad del sistema, los niveles de gestión necesarios cuando cambia el sistema, la asignación de presupuestos financieros y el control y distribución del software.

La norma ISO 20000 se denominó anteriormente BS 15000 y está alineada con el planteamiento del proceso definido por la IT Infrastructure Library (ITIL - Biblioteca de infraestructuras de tecnología de la información) de The Office of Government Commerce (OGC).

LAS VENTAJAS DE LA NORMA ISO 20000

La reputación de la ISO y el reconocimiento internacional del IT Service Management System (Sistema de gestión de servicios de tecnología de la información) que conlleva la norma ISO 20000 es un verdadero refuerzo para la reputación de cualquier empresa. Reduce el riesgo ofreciendo apoyo fiable de profesionales de la tecnología de la información (internos o subcontratados), cuándo y dónde más se necesita. Esto ayuda a poner cualquier situación de tecnología de la información bajo control inmediato y disminuye sus daños potenciales, mejorando la productividad de los empleados y la fiabilidad del sistema de tecnología de la información. Y lo que es más, la certificación aporta motivación a la organización y demuestra la fiabilidad y calidad de los servicios de tecnología de la información para empleados, partes interesadas y clientes.

La certificación de su Sistema de gestión de servicios de tecnología de información a través de SGS ayudará a su organización a desarrollar y mejorar su rendimiento.

- Su certificado IT Service Management System según la norma ISO 20000 de SGS le permitirá demostrar altos niveles de calidad y fiabilidad de los servicios de tecnología de información, cuando presente ofertas para

contratos internacionales o cuando realice ampliaciones locales para aumentar su volumen de negocio.

- La evaluación periódica realizada por SGS le ayudará a utilizar, supervisar y mejorar continuamente su sistema de gestión de los servicios de tecnología de la información y sus procesos. Esto mejorará la fiabilidad de sus operaciones internas para satisfacer las necesidades de los clientes y también para aumentar su rendimiento global. Lo más probable es que también consiga una mejora importante en motivación, compromiso y comprensión de su responsabilidad por parte del personal.
- La norma ISO 20000 se puede vincular también con la norma ISO 27000 (norma internacional para seguridad de la información). Integrando las auditorías de estos sistemas de gestión podrá ahorrar tiempo y dinero.

ESTRUCTURA

En la introducción hay una frase que llama la atención: "Los servicios y la gestión de estos servicios son esenciales para ayudar a las organizaciones a generar ingresos y ser rentables". Es decir, a esta altura del siglo ninguna organización puede dudar más, que todo proceso o aplicación informática, es una de las principales fuentes de dinero para la empresa.

Se trata de una norma eminentemente basada en procesos, y a lo largo de su desarrollo, especifica trece de ellos, agrupados en seis grupos que se corresponden a los puntos 5 al 10 del estándar.

El **punto 1**, que habla del objetivo y alcance de esta norma, establece que la misma puede ser aplicada en empresas que solicitan ofertas o desean un enfoque consistente con sus proveedores de servicio, por los mismos proveedores para medir su eficiencia o demostrarla, como base para una evaluación independiente, o por cualquier organización que desee mejorar sus propios servicios.

De todo esto, es muy importante recalcar que el ámbito más genérico estará siempre bajo el enfoque de "Servicios".

El **punto 2** se refiere a definiciones, y los **puntos 3 y 4** se refieren al Sistema de gestión. Cubren desde el compromiso de la Dirección, hasta los documentos procesos y la formación. Luego pasa con buen nivel de detalle al ciclo PDCA (Plan-Do-check-Act).

El **punto 5** describe la planificación e implementación de nuevos servicios o servicios modificados, sin entrar en mucho detalle.

A partir del punto 6 y hasta el 10 es donde describe la implementación de estos seis grupos de procesos, cuyo temario referimos a continuación.

Punto 6. Procesos para la provisión del servicio. Incluye: Gestión del nivel del servicio, Generación de informes de servicio, Gestión de la continuidad y disponibilidad del servicio, Elaboración de presupuesto y contabilidad de los servicios de TI, Gestión de la capacidad y Gestión de la seguridad de la información.

Objetivos del punto 6: Planificación, diseñar, dimensionar, generar, valorar económicamente y asegurar la provisión de un servicio.

Punto 7. Procesos de relaciones. Comprende: Gestión de las relaciones con el negocio y Gestión de suministradores

Objetivos del punto 7: Establecer un marco de buena colaboración entre el cliente y el proveedor, garantizando las mejores condiciones.

Punto 8. Procesos de resolución. Este punto trata dos aspectos: Gestión del incidente y Gestión del problema, los cuales a pesar de estar íntimamente relacionados son procesos separados.

Objetivos del punto 8: Minimizar problemas y en caso de producirse, restaurarlos lo antes posible.

Punto 9. Procesos de control. Comprende dos procesos: Gestión de configuración y Gestión del cambio

Objetivos del punto 9: Detallar al máximo todos los procesos implementados, mantenerlos actualizados con información precisa y planificar cambios para asegurar su estabilidad.

Punto 10. Proceso de entrega. Se refiere exclusivamente a la Gestión de la entrega

Objetivos del punto 10: Su finalidad es la de regular toda la actividad de entrega para los entornos en producción, el seguimiento, los plazos, posibilidades de marcha atrás, entornos de prueba, y las mediciones de éxito y fallo de las mismas.

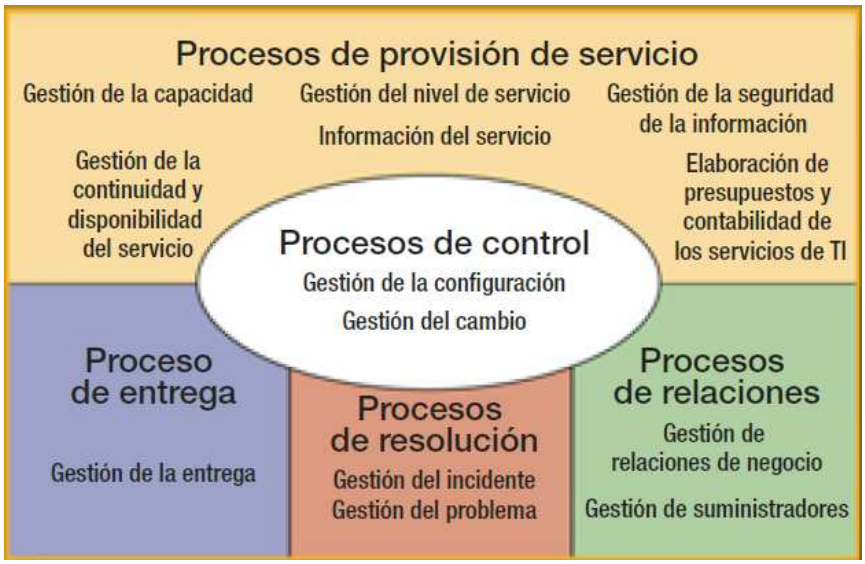


Imagen 15: Procesos de gestión de servicios de la norma ISO 20000

PROPÓSITO

El propósito de ISO 20000 es proveer una norma de referencia común para toda empresa que ofrezca servicios de TI tanto a clientes internos como externos. Ya que la comunicación juega un papel esencial en la gestión de servicio, uno de los objetivos más importantes de la norma es crear una terminología común para las organizaciones proveedoras de servicio TI, sus suministradores y sus clientes.

Esta norma se establece para definir todo aquello que es obligatorio para la buena gestión de servicios (aspectos comunes y requeridos para toda la buena gestión de servicios) y no para especificar directamente requisitos particulares.

La recopilación de la información clave de los procesos de gestión de servicio de ITIL en una norma ISO internacional formalizada, permite a los proveedores de servicio TI decidir su adecuación de manera formal a estas mejores prácticas.

En específico, la parte concerniente a Especificaciones está compuesta por un conjunto amplio de requerimientos orientados a garantizar una administración de servicios de TI de calidad. A continuación se listan junto a sus objetivos

Requerimientos para un sistema de gestión: Proporcionar un sistema de gestión, incluyendo políticas y un marco de referencia para permitir la gestión e implementación efectiva de todos los servicios de TI.

Planeación e implementación de la gestión de servicios: Planear la implementación y entrega de la gestión de servicios; Implantar el plan y los objetivos de la gestión de servicios; Monitorear, medir y revisar que el plan y los objetivos de gestión de los servicios estén siendo alcanzados; Mejorar la efectividad y eficiencia de la entrega y gestión del servicio.

Planeación e implementación de servicios nuevos o modificados: Asegurar que los nuevos servicios y cambios hechos a los servicios puedan ser entregados y administrados a un costo y calidad de servicio adecuados.

Proceso de entrega del servicio: Definir, acordar, registrar y administrar los niveles de servicio; Desarrollar informes concertados, oportunos, confiables y precisos, para la toma informada de decisiones y la comunicación efectiva; Asegurar que las obligaciones acordadas con los clientes pueden ser satisfechas en todas las circunstancias; Presupuestar y contabilizar el costo de la provisión del servicio; Asegurar que la organización cuenta, en cualquier momento, con la capacidad suficiente para satisfacer la demanda actual y futura acordada del negocio, Administrar la seguridad de la información de forma efectiva dentro de todas las actividades de servicio.

Procesos de relación: Establecer y mantener una buena relación entre el proveedor de servicio y el cliente, basada en el entendimiento del cliente y sus conductas de negocio, Gestionar a los proveedores externos para asegurar una provisión de servicios limpia y de calidad.

Procesos de resolución: Restablecer el servicio acordado en el negocio lo más rápidamente posible, o responder a las solicitudes de servicio; Minimizar las interrupciones para el negocio a través de la identificación y análisis proactivo de la causa de los incidentes del servicio y la gestión del cierre de incidentes.

Procesos de control: Definir y controlar los componentes del servicio y la infraestructura, y mantener información precisa de la configuración; Asegurar que todos los cambios sean evaluados, aprobados, implementados y revisados de una forma controlada.

Procesos de software: Entregar, distribuir y rastrear uno o más cambios en una liberación lanzada al ambiente real.

Resumiendo:

- Alineación de los servicios de TI y la estrategia de negocios.
- Se crea un marco de trabajo formal para proyectos de mejora del servicio.
- Crea ventajas competitivas a través de la promoción de servicios consistentes y al menor costo posible.
- Por requerir propietarios y responsabilidad a todos los niveles, crea una cultura y filosofía de progreso.
- Reducción del riesgo y así los costos de los servicios externos recibidos.
- Mejora la reputación y la percepción.

Refiriéndonos específicamente a la industria de la informática ¿Qué hace el estándar global ISO/IEC 20000 por la Administración de Servicios de TI?

- Ofrece una base de comparación independiente.
- Proporciona un estándar de comparación que aplica a todos los proveedores de servicio independientemente del país, lenguaje, sector, tamaño y localización.
- Actúa como punto de partida para otras mejoras.
- Ofrece insumos para la actualización de ITIL.

¿QUÉ ENCONTRAMOS EN COMÚN CON LA ISO 27000?

Sobre todo, y lo más importante es la fuerte orientación que hacen hacia la gestión a través del compromiso de la Dirección, para seguir avanzando en el ciclo PDCA. Debemos recordar que las dos grandes diferencias entre ISO 17799 e ISO 27001, fueron la inclusión del Análisis de Riesgo y el ciclo PDCA (presentado bajo la forma de SGSI).

La eminente orientación a procesos, también es un denominador común, pues en la ISO-27001, cada uno de los controles que propone, hace mención a que debe ser "auditable", para permitir con ello verificar su evolución, lo cual no es nada menos que un proceso continuo.

Muchos de los procesos que propone ISO 20000, forman parte de un "mensaje subliminal" u oculto hacia seguridad, pues la disponibilidad, las incidencias, la recuperación, los contratos, las pruebas de maqueta, la continuidad, los registros, etc., son temas que incluye también ISO 27000.

Las referencias a "disponibilidad" aparecen 32 veces en ambas partes de ISO 20000, mientras que "Integridad" aparece 4 veces, y "Confidencialidad" no aparece ninguna. Estas cuentas, aunque parezcan triviales, no lo son, pues nos están dejando la evidente intención que tiene la norma, es decir la "DISPONIBILIDAD" de los servicios.

Nos atreveríamos casi a asegurar, que la "Seguridad", luego de la Gestión (y en ese orden) es el pilar más robusto de la "Gestión de Servicio".

CONCLUSIONES

ISO 20000 está orientada exclusivamente a Gestionar Servicios. Por lo tanto hay que evaluar qué porcentaje de los procesos de negocio de la empresa están muy relacionados con servicios, si esta tasa es baja, no es una buena decisión ponerse a trabajar con ISO 20000.

Hay Servicios, y servicios..... Si los mismos, tienen importante relación con la seguridad, datos íntimos, financieros, policiales, I+D, estratégicos, etc. (Ejemplo: Aseguradoras, banca, industria farmacológica o petrolera, Justicia, policial, etc.). La mejor opción sería comenzar pensando en ISO 27001. Si los Servicios no procesan información tan clasificada, dependen de un alto volumen de transacciones, la "confidencialidad e Integridad" no son los parámetros cruciales, etc. (Ejemplo: centros de venta, control de stock, almacenaje, fabricación en serie, etc.) un buen camino es ISO 20000.

Si la empresa es prestadora de servicios, ISO 20000 es importante como señal de seriedad y esfuerzo, si esos servicios están orientados a empresas cuyos procesos guardan relación con "Confidencialidad e Integridad", entonces cuidado con ISO 27001.

Si la magnitud de la empresa es pequeña (Pymes), ISO 20000 no es tan sencillo y por el contrario, si lo es ISO 27001.

Si aún no se han iniciado metodologías de gestión y calidad, antes de plantearse cuál de los dos, lo importante es plantearse PDCA, bajo cualquier familia.

RELACIÓN CON ITIL

ISO 20000 está alineada con el marco de trabajo de la Biblioteca de Infraestructura de TI (ITIL) definido en los volúmenes de Soporte de Servicio y Provisión de Servicio. ITIL es un conjunto de mejoras prácticas, mientras que ISO 20000 es un conjunto formal de especificaciones cuyo cumplimiento debería ser perseguido por los proveedores de servicios: ser capaces de proveer servicios de alta calidad. Aplicar las mejores prácticas de la Biblioteca de Infraestructura de TI ayudará al proveedor de servicio a alcanzar la calidad en la gestión de servicio requerida por ISO 20000.

La relación entre ISO 20000 e ITIL se puede observar en la siguiente imagen:

Imagen 16: Relación entre ISO 20000 e ITIL

APÉNDICE D: GESTIÓN DE SERVICIO TI

GESTION DE SERVICIO TI

La Gestión de servicios de tecnologías de la información (TI) de alta calidad (ITSM) es una disciplina que se basa en procesos, enfocados en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

Usualmente la gestión de servicios de TI involucra el uso de outsourcings, insourcings y servicios compartidos. Es extremadamente importante mantener una base de conocimiento amplia dentro de la organización para que estas prácticas sean exitosas.

Los objetivos de una buena gestión de servicios TI han de ser:

- Proporcionar una adecuada gestión de la calidad
- Aumentar la eficiencia
- Alinear los procesos de negocio y la infraestructura TI
- Reducir los riesgos asociados a los Servicios TI
- Generar negocio

1. Alineación con los objetivos del negocio

Las organizaciones actuales realizan inversiones importantes en recursos de tecnología de información para así apoyar los procesos de negocio. El valor significativo y relevante que el uso de la información tiene para las organizaciones, determina que todos los procesos relativos a la producción, administración y uso de servicios de Tecnologías de Información (TI) deben ser óptimamente gestionados y controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio. Los procesos de datos e información producto de las operaciones y procesos del negocio, requieren la aplicación de técnicas y medidas de control en el marco de un sistema de gestión que garantice la prestación de los servicios y la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema operacional, organizacional y del sistema macro del negocio. Todo lo anterior, justifica la necesidad de optimizar los recursos de TI en apoyo y alineación con los objetivos de negocio a través de procesos efectivos de GESTIÓN DE SERVICIO TI.

En las organizaciones existe una organización de TI que genera y provee los servicios de TI y un grupo de clientes internos (usuarios) y externos que demandan esos servicios y esperan su prestación oportuna y con calidad. Las relaciones y comunicaciones entre el proveedor de TI y los clientes de TI deben ser canalizadas a través de un sistema que garantice la optimación de los procesos de entrega y soporte de servicios a través de la consolidación de Gestión de Servicio TI. Las inversiones en la infraestructura de TI y en los activos de información de las organizaciones cada vez son más importantes, lo cual justifica la implantación de sistemas que aseguren el rendimiento de los procesos basados en servicios de TI para asegurar la reducción del costo total de propiedad (TCO) y un retorno de la inversión (ROI) razonable. Hasta ahora, sólo algunas empresas de alto nivel y tamaño han asumido e incorporado a su cultura organizacional y planes de negocio, los procesos de Gestión de Servicio TI basada en las mejores prácticas de aceptación internacional. Este nuevo paradigma basado en el servicio debe tener un acercamiento a las Organizaciones de cualquier tamaño, las empresas deben adoptar y

adaptar estas mejores prácticas bajo un enfoque de Calidad de Servicio y oportunidad para el cambio del negocio con la aplicación de estándares actualizados. Este paradigma se fundamenta en el mejoramiento continuo de la Cultura de Servicio TI.

Los productos y servicios de estos marcos de referencia están orientados a la implantación de sistemas consolidados de mejoramiento continuo en la Gestión de Servicio de Tecnología de Información en alineación con los objetivos del negocio, de punta a punta desde las fases diagnóstica y de planificación hasta la implantación, monitoreo, supervisión y optimación. La tendencia de Gestión de Servicio TI se basa en la promoción y soporte de aplicación de las mejores prácticas, marcos referenciales y estándares de aceptación internacional, tales como ISO/IEC 20000, ITIL, ITSCMM, COBIT, ISO/IEC -17799 – 2700X, y otras.

2. Gobierno de las TI

La Gestión de Gobierno de TI, traducción del conjunto de mejores prácticas establecidas como ITSM del inglés (Information Technology Service Management) acuñado a partir de la creación e implantación de los principios y fundamentos ingleses promovidos en el conjunto de prácticas documentadas en ITIL (Information Technology Infraestructure Library), normados en el código BS15000 (British Standard 15000) y que actualmente se ha internacionalizado y estandarizado a nivel global por la extensión en la norma ISO/IEC 20000, es hoy día un nuevo y vigoroso enfoque de prácticas a seguir y base de certificación en esquemas de negocio de mejoramiento continuo en el uso y aprovechamiento de Tecnologías de Información en apoyo al logro de los objetivos de negocio.

Se pueden crear relaciones entre los procesos, actividades, roles, empleados y sistemas TI, ya sean procesos ITIL o procesos ISO 20000. Además, la biblioteca ITIL (V2 y V3) contiene un modelo de roles que permite deducir los conocimientos necesarios de los empleados y definir una estructura organizativa adecuada en cada caso. A continuación se detallan, uno a uno, tanto procesos ITIL como procesos ISO 20000:

- *ITIL V3: El Ciclo de Vida del Servicio.*

Los procesos ITIL v3 son conjuntos estructurados de actividades diseñados para cumplir un objetivo concreto. De este modo, los procesos ITIL v3 requieren de una o más entradas y producen una seria de salidas, ambas definidas con anterioridad. Los procesos ITIL v3 suelen incorporar la definición de los roles que intervienen, las responsabilidades, herramientas y controles de gestión necesarios para obtener las salidas de forma eficaz. Los procesos ITIL v3 siguientes definen las políticas, estándares, guías de actuación, actividades e instrucciones de trabajo necesarias para una correcta gestión de los servicios TI.

- *ITIL V2: Soporte y Provisión de Servicios TI*

ITIL V2 está especialmente desarrollada para reducir los costos de provisión y soporte de los servicios IT al mismo tiempo que garantiza los requerimientos de la información en cuanto a seguridad y mantiene e incrementa los niveles de fiabilidad, consistencia y calidad de su negocio. De esta manera permite alinear la provisión y el soporte de los servicios de TI con las necesidades de la empresa.

- *ISO 20000: Norma para la Gestión de Servicios TI*

La norma ISO 20000 se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia. La norma considera también la capacidad del sistema, los niveles de gestión necesarios cuando cambia el sistema, la asignación de presupuestos financieros y el control y distribución del software.

APÉNDICE E: APLICACIÓN: CUESTIONARIO ISO 20000

APÉNDICE E: APLICACIÓN: CUESTIONARIO ISO 20000

ESPECIFICACIONES FUNCIONALES

Se ha desarrollado una aplicación que consiste en un cuestionario que el usuario rellenará.

El cuestionario consta de dieciséis preguntas, con cinco posibles respuestas alternativas (siempre, a menudo, con frecuencia, a veces y nunca).

El usuario marcará una de las cinco posibles respuestas para cada pregunta, y con las respuestas dadas se calculará un porcentaje de cumplimiento de la ISO 20000 en la organización. Por defecto, la respuesta siempre viene marcada con la opción SIEMPRE.

El desarrollo de la aplicación se ha llevado a cabo en SAP, en el lenguaje de programación ABAP4, en el módulo FI.

Se ha elegido este lenguaje ya que es gráfico e intuitivo para la utilización del usuario.

Para ejecutar la aplicación, será necesario tener instalado el SAP GUI.

Una vez dentro del SAP, se llama a la transacción ZCUESTIONARIO, que lanza directamente el cuestionario.

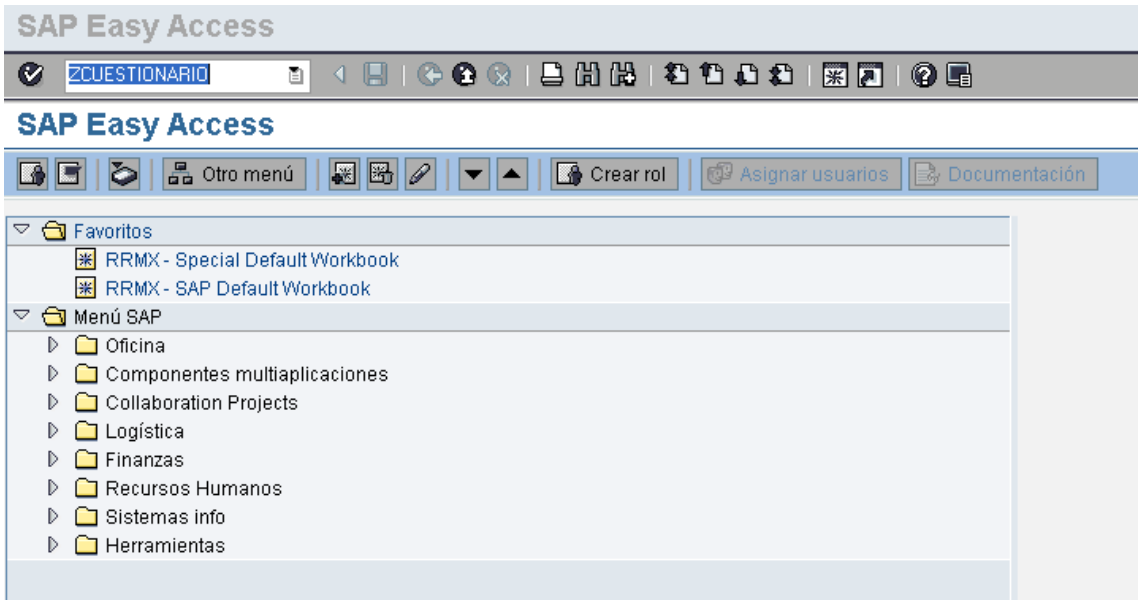


Imagen 17: Cuestionario ISO 20000: Transacción.

El título de la aplicación es: Cuestionario ISO 20000.

La barra de herramientas tiene los botones back, exit y cancel, que permiten salir de la aplicación.

El status tiene el botón siguiente, que permite continuar para seguir respondiendo a las preguntas.

Al pulsar el botón SIGUIENTE aparece la siguiente pantalla.

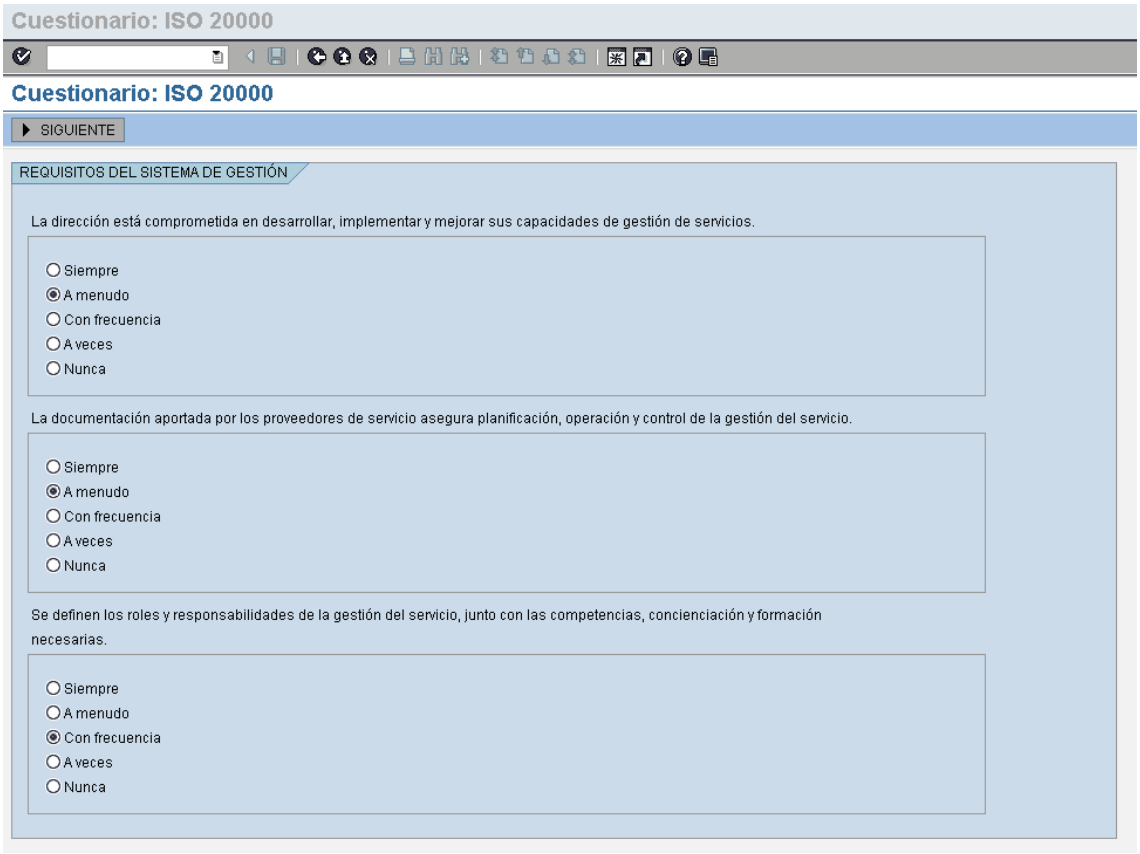


Imagen 18: Cuestionario ISO 20000: Requisitos del sistema de gestión.

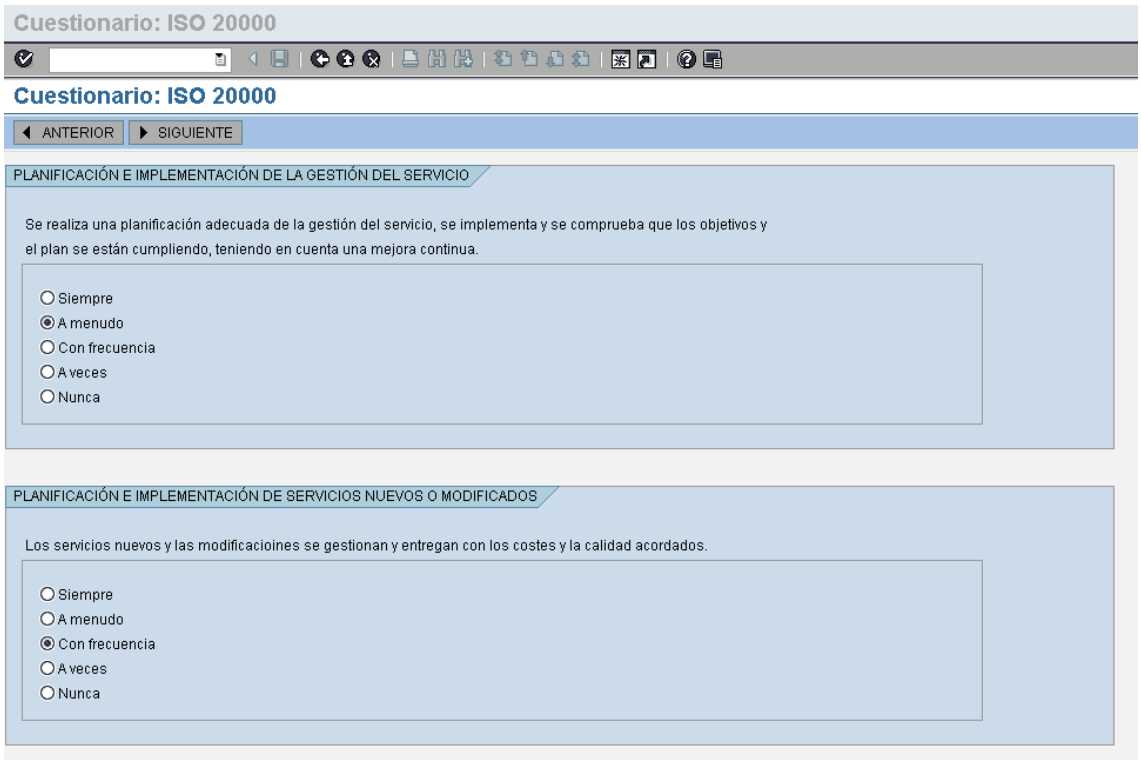


Imagen 19: Cuestionario ISO 20000: Planificación e implementación de la gestión del servicio y planificación e implementación de servicios nuevos o modificados.

Ahora aparecen los botones SIGUIENTE y ANTERIOR, que permiten, o bien continuar con las preguntas o volver a la pantalla anterior para rectificar alguna respuesta.

Estos botones aparecerán en todas las ventanas, excepto en la última.

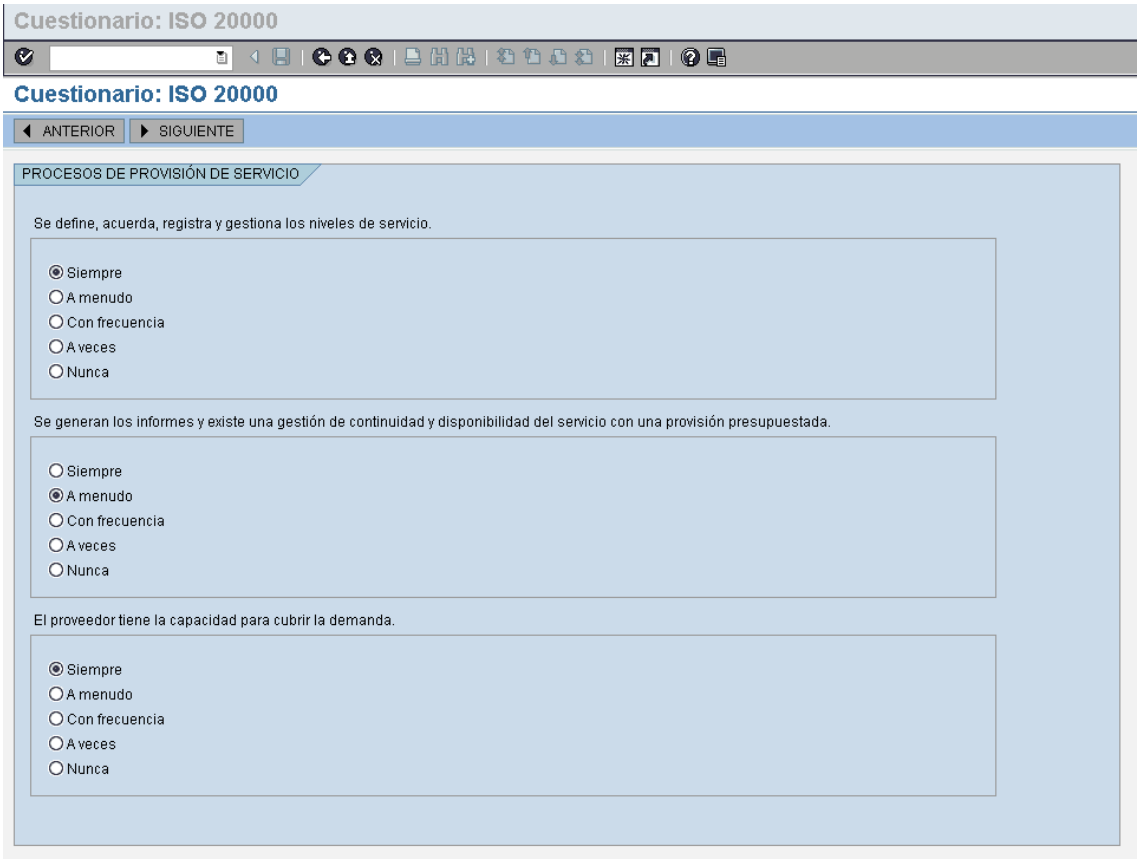


Imagen 20: Cuestionario ISO 20000: Procesos de provisión de servicio.

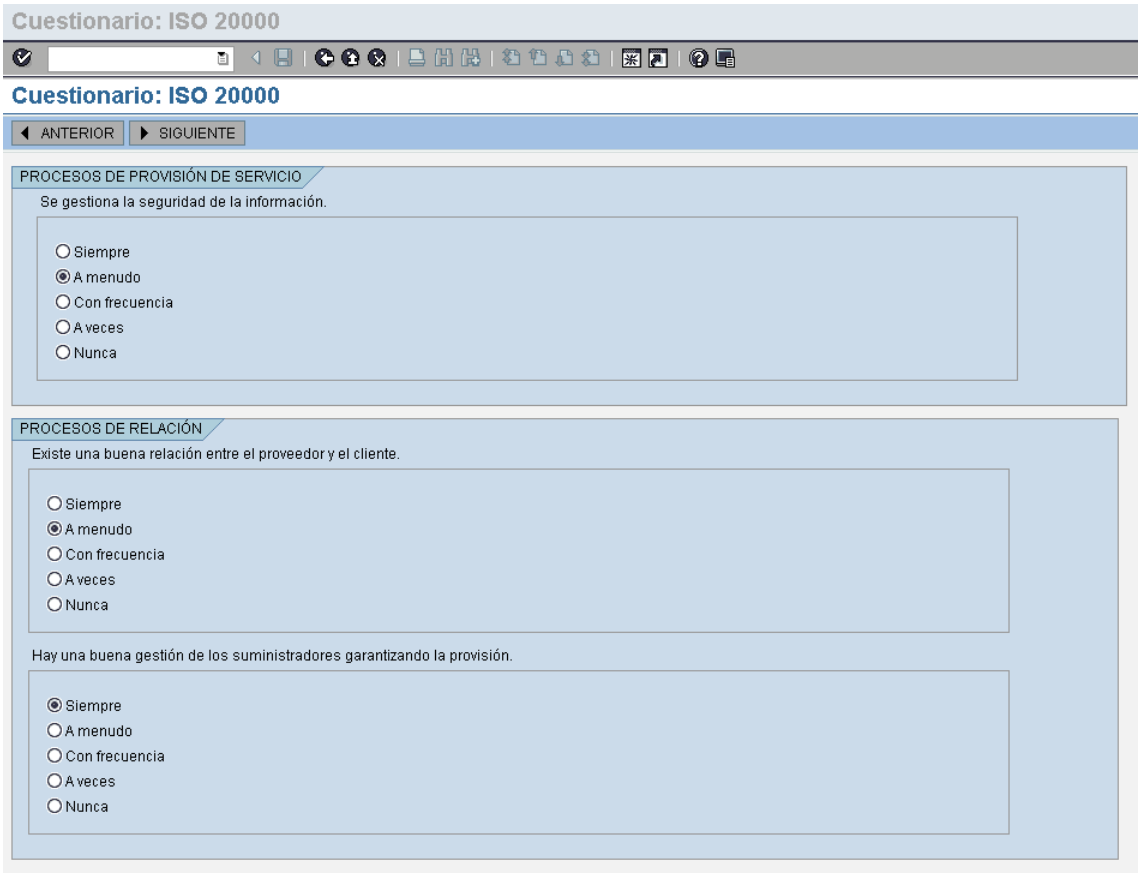


Imagen 21: Cuestionario ISO 20000: Procesos de provisión de servicio y procesos de relación.

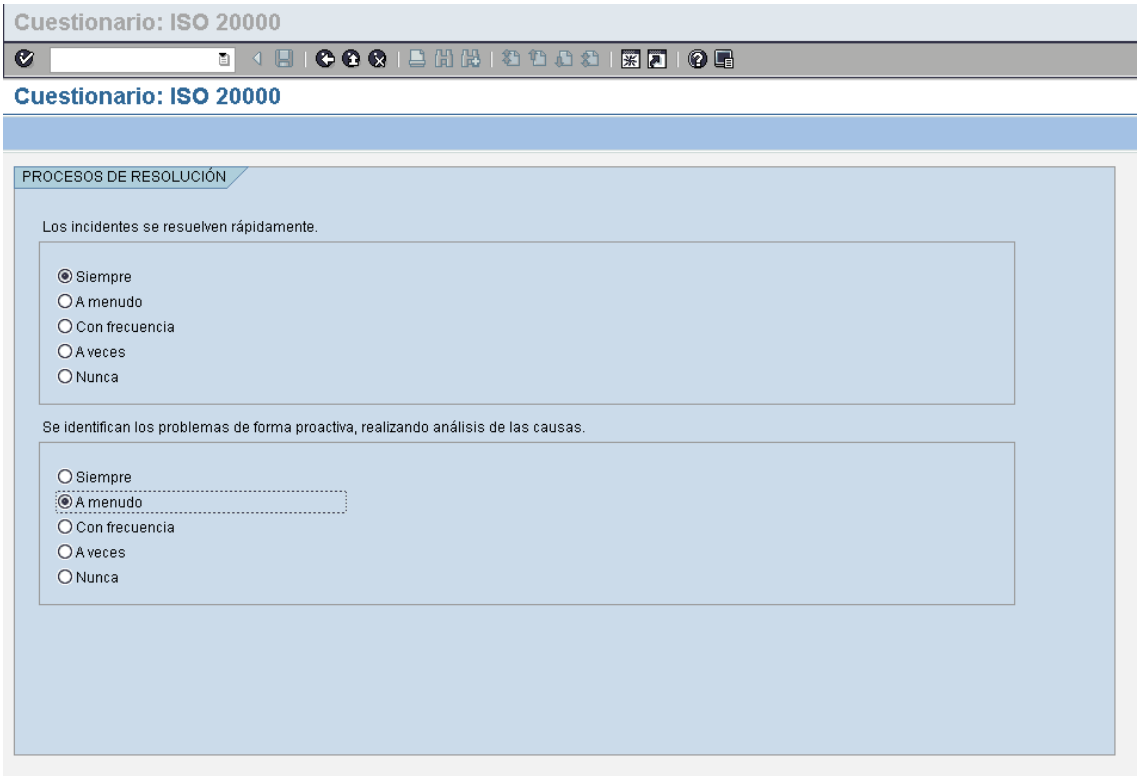


Imagen 22: Cuestionario ISO 20000: Procesos de resolución.

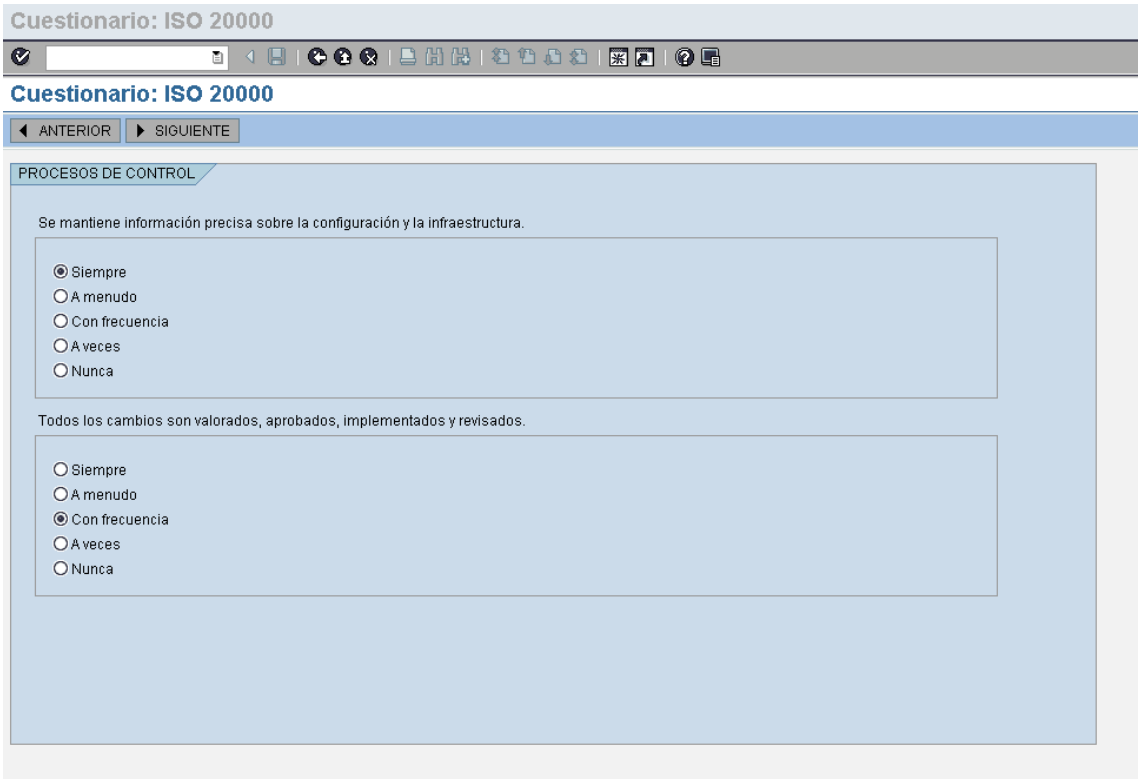


Imagen 23: Cuestionario ISO 20000: Procesos de control.

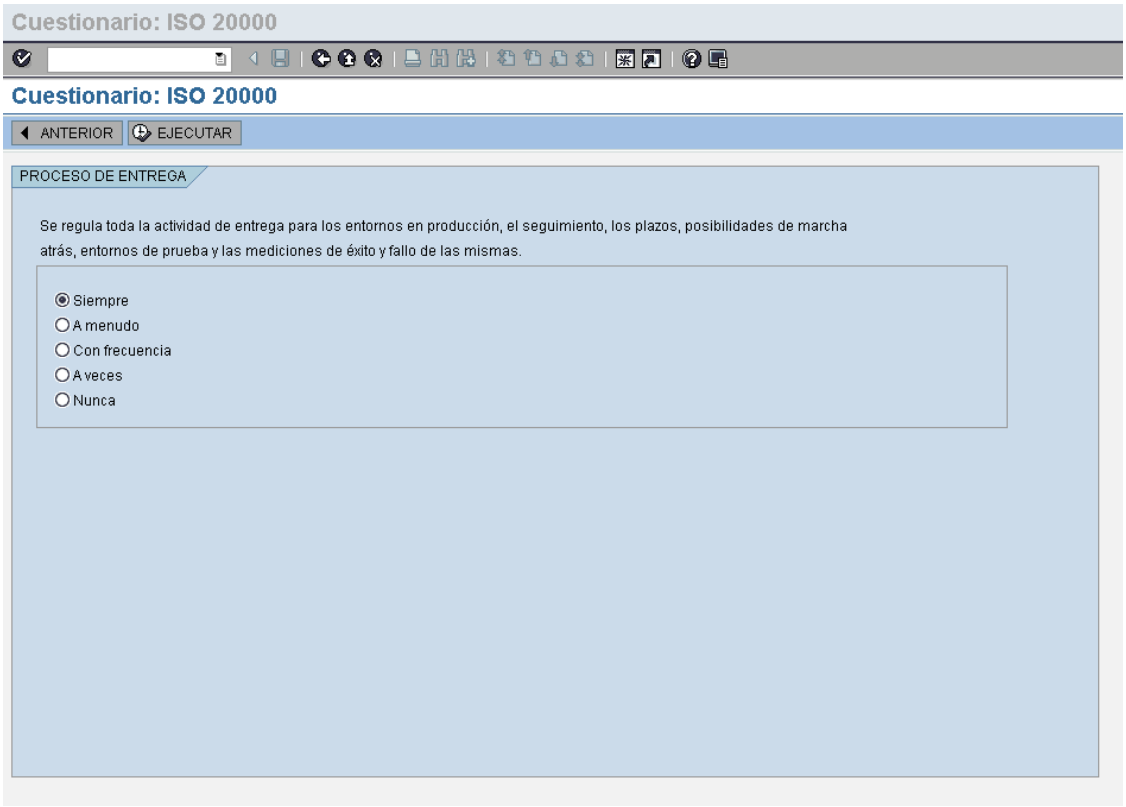


Imagen 24: Cuestionario ISO 20000: Proceso de entrega.

Se puede observar que ahora aparece el botón EJECUTAR, ya que estamos en la última pregunta del cuestionario. Al pulsar el botón, aparece la siguiente pantalla.

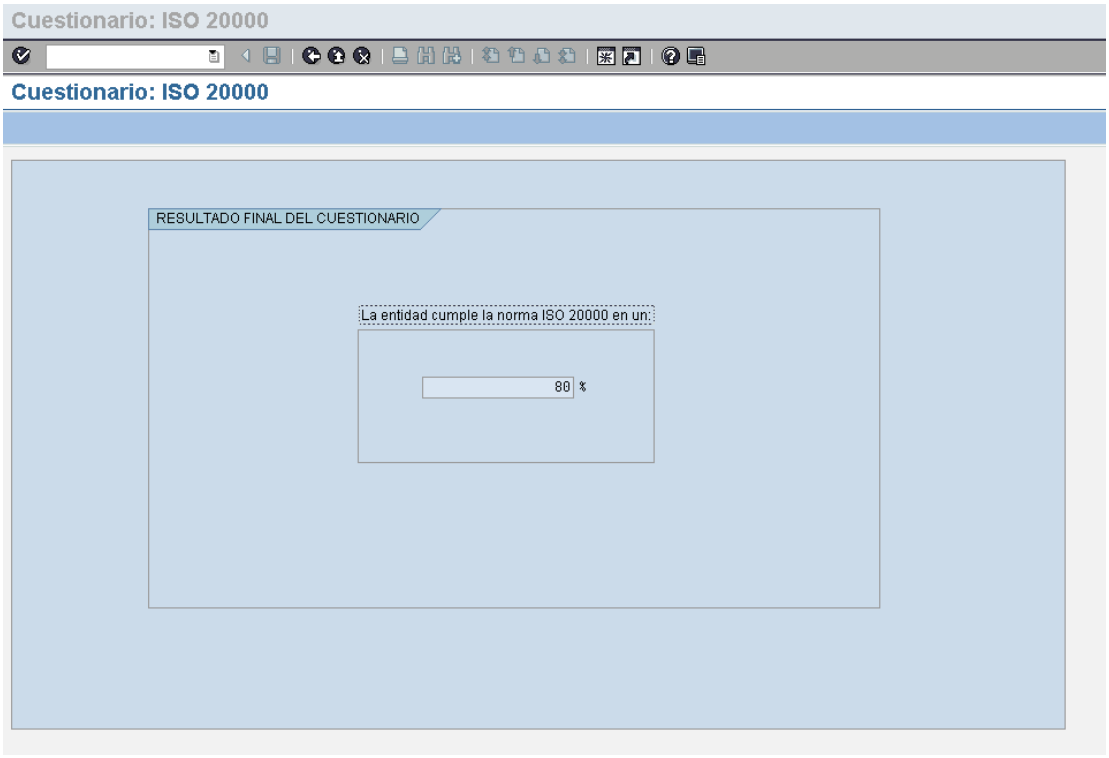


Imagen 25: Cuestionario ISO 20000: Resultado final.

En este ejemplo ficticio, la entidad tendría un 80 % de cumplimiento.

ESPECIFICACIONES TÉCNICAS

NOMBRE DEL PROGRAMA:	ZCUESTIONARIO
Título:	Cuestionario ISO 20000.
Relación con otros Desarrollos:	
Transacciones SAP / Z dónde se utiliza:	ZCUESTIONARIO
Clase de Desarrollo:	
Tipo de Desarrollo: (Module – Pool / Report)	Report

Tabla 15: Especificaciones técnicas

Objetos Z		
Tipo (TABLAS, ESTRUCTURAS, MÓDULOS DE FUNCIONES, INCLUDES, ETC)	**Nombre**	**Descripción**
Programa	ZCUESTIONARIO	Contiene los includes.
Include	ZCUESTIONARIO_TOP	Declaraciones de variables, tablas y constantes.
Include	ZCUESTIONARIO_SEL	Pantalla de selección.
Include	ZCUESTIONARIO_F01	Contiene las subrutinas.
Include	ZCUESTIONARIO_IO0	Contiene los módulos.

Tabla 16: Especificaciones técnicas – objetos z

CÓDIGO DEL PROGRAMA

PROGRAMA PRINCIPAL

```
*&---------------------------------------------------------------------*
*& Module Pool       ZCUESTIONARIO
*&
*&---------------------------------------------------------------------*
*&
*&
*&---------------------------------------------------------------------*
*  Calcula el porcentaje de cumplimiento de la norma ISO 20000
*&---------------------------------------------------------------------*
PROGRAM  ZCUESTIONARIO.

INCLUDE ZCUESTIONARIO_TOP.
INCLUDE ZCUESTIONARIO_IO0.
INCLUDE ZCUESTIONARIO_SEL.

************************************************************************
* Proceso principal
************************************************************************
START-OF-SELECTION.
  CALL SCREEN 100.

INCLUDE ZCUESTIONARIO_F01.
```

INCLUDE ZCUESTIONARIO_F01

```
*&---------------------------------------------------------------------*
*&  Include           ZCUESTIONARIO_F01
*&---------------------------------------------------------------------*

*&---------------------------------------------------------------------*
*&      Form  USER_COMMAND_0100
*&---------------------------------------------------------------------*
FORM USER_COMMAND_0100 .

CASE sy-ucomm.
    WHEN 'BACK' OR 'END' OR 'CANC'.
      LEAVE PROGRAM.
    WHEN 'SIG'.
      IF d_cont = 1.
        CALL SCREEN 110.
      ELSEIF d_cont = 2.
        CALL SCREEN 120.
      ELSEIF d_cont = 3.
        CALL SCREEN 130.
      ELSEIF d_cont = 4.
        CALL SCREEN 140.
      ELSEIF d_cont = 5.
        CALL SCREEN 150.
      ELSEIF d_cont = 6.
        CALL SCREEN 160.
      ENDIF.
    WHEN 'ANT'.
      IF d_cont = 2.
        CALL SCREEN 100.
      ELSEIF d_cont = 3.
        CALL SCREEN 110.
      ELSEIF d_cont = 4.
        CALL SCREEN 120.
      ELSEIF d_cont = 5.
        CALL SCREEN 130.
      ELSEIF d_cont = 6.
        CALL SCREEN 140.
      ELSEIF d_cont = 7.
        CALL SCREEN 150.
      ENDIF.

   WHEN 'EJECUTAR'.
     PERFORM realizar_calculo.

  ENDCASE.

ENDFORM.                    " USER_COMMAND_0100

*&---------------------------------------------------------------------*
*&      Form  REALIZAR_CALCULO
*&---------------------------------------------------------------------*
FORM REALIZAR_CALCULO .

DATA: d_por type i.

CLEAR: d_por, d_total.
```

```
* BLOQUE 1*
* PRIMERA PREGUNTA *
IF p_r111 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r112 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r113 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r114 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r115 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r121 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r122 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r123 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r124 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r125 = 'X'.
  d_por = d_por + 0.
ENDIF.

* TERCERA PREGUNTA *
IF p_r131 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r132 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r133 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r134 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r135 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 2 *
* PRIMERA PREGUNTA *
IF p_r211 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r212 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r213 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r214 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r215 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 3 *
* PRIMERA PREGUNTA *
IF p_r311 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r312 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r313 = 'X'.
```

```
  d_por = d_por + 50.
ELSEIF p_r314 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r315 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 4 *
* PRIMERA PREGUNTA *
IF p_r411 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r412 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r413 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r414 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r415 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r421 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r422 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r423 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r424 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r425 = 'X'.
  d_por = d_por + 0.
ENDIF.

* TERCERA PREGUNTA *
IF p_r431 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r432 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r433 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r434 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r435 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r441 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r442 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r443 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r444 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r445 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 5 *
```

```
* PRIMERA PREGUNTA *
IF p_r511 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r512 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r513 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r514 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r515 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r521 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r522 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r523 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r524 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r525 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 6 *
* PRIMERA PREGUNTA *
IF p_r611 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r612 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r613 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r614 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r615 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r621 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r622 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r623 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r624 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r625 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 7 *
* PRIMERA PREGUNTA *
IF p_r711 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r712 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r713 = 'X'.
  d_por = d_por + 50.
```

```
ELSEIF p_r714 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r715 = 'X'.
  d_por = d_por + 0.
ENDIF.

* SEGUNDA PREGUNTA *
IF p_r721 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r722 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r723 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r724 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r725 = 'X'.
  d_por = d_por + 0.
ENDIF.

* BLOQUE 8 *
* PRIMERA PREGUNTA *
IF p_r811 = 'X'.
  d_por = d_por + 100.
ELSEIF p_r812 = 'X'.
  d_por = d_por + 75.
ELSEIF p_r813 = 'X'.
  d_por = d_por + 50.
ELSEIF p_r814 = 'X'.
  d_por = d_por + 25.
ELSEIF p_r815 = 'X'.
  d_por = d_por + 0.
ENDIF.

d_total = d_por / 16.
v_resultado = d_total.
SHIFT v_resultado LEFT DELETING LEADING ' '.
CALL SCREEN 170.

ENDFORM.                    " REALIZAR_CALCULO
```

INCLUDE ZCUESTIONARIO_IO0

```
*&---------------------------------------------------------------------*
*&  Include           ZCUESTIONARIO_IO0
*&---------------------------------------------------------------------*

*&---------------------------------------------------------------------*
*&      Module  USER_COMMAND_0100  INPUT
*&---------------------------------------------------------------------*
MODULE USER_COMMAND_0100 INPUT.

PERFORM user_command_0100.

ENDMODULE.                 " USER_COMMAND_0100  INPUT
```

```
*&---------------------------------------------------------------------*
*&      Module  STATUS_0100  OUTPUT
*&---------------------------------------------------------------------*
MODULE STATUS_0100 OUTPUT.

  SET PF-STATUS 'ST100'.
  SET TITLEBAR 'TITLE100'.

ENDMODULE.                 " STATUS_0100  OUTPUT


*&---------------------------------------------------------------------*
*&      Module  STATUS_0110  OUTPUT
*&---------------------------------------------------------------------*
MODULE STATUS_0110 OUTPUT.

  SET PF-STATUS 'ST110'.
  SET TITLEBAR 'TITLE100'.

ENDMODULE.                 " STATUS_0110  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  STATUS_0170  OUTPUT
*&---------------------------------------------------------------------*
MODULE STATUS_0170 OUTPUT.

  SET PF-STATUS 'ST170'.
  SET TITLEBAR 'TITLE100'.

ENDMODULE.                 " STATUS_0170  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  STATUS_0160  OUTPUT
*&---------------------------------------------------------------------*
MODULE STATUS_0160 OUTPUT.

  SET PF-STATUS 'ST160'.
  SET TITLEBAR 'TITLE100'.

ENDMODULE.                 " STATUS_0160  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO OUTPUT.
  d_cont = 1.
ENDMODULE.                 " NUM_DYMPRO  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO110  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO110 OUTPUT.
  d_cont = 2.
ENDMODULE.                 " NUM_DYMPRO110  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO120  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO120 OUTPUT.
  d_cont = 3.
ENDMODULE.                 " NUM_DYMPRO120  OUTPUT
```

```
*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO130  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO130 OUTPUT.
  d_cont = 4.
ENDMODULE.                 " NUM_DYMPRO130  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO140  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO140 OUTPUT.
  d_cont = 5.
ENDMODULE.                 " NUM_DYMPRO140  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO150  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO150 OUTPUT.
  d_cont = 6.
ENDMODULE.                 " NUM_DYMPRO150  OUTPUT

*&---------------------------------------------------------------------*
*&      Module  NUM_DYMPRO160  OUTPUT
*&---------------------------------------------------------------------*
MODULE NUM_DYMPRO160 OUTPUT.
  d_cont = 7.
ENDMODULE.                 " NUM_DYMPRO160  OUTPUT
```

INCLUDE ZCUESTIONARIO_SEL

```
*&---------------------------------------------------------------------*
*&  Include           ZCUESTIONARIO_SEL
*&---------------------------------------------------------------------*

**********************************************************************
***** Pantalla de selección
**********************************************************************

* BLOQUE 1 *
SELECTION-SCREEN BEGIN OF SCREEN 200 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b1 WITH FRAME TITLE text-001.
PARAMETERS: p_r111 RADIOBUTTON GROUP g1,
            p_r112 RADIOBUTTON GROUP g1,
            p_r113 RADIOBUTTON GROUP g1,
            p_r114 RADIOBUTTON GROUP g1,
            p_r115 RADIOBUTTON GROUP g1.
SELECTION-SCREEN END OF BLOCK b1.
SELECTION-SCREEN END OF SCREEN 200.

SELECTION-SCREEN BEGIN OF SCREEN 300 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b2 WITH FRAME TITLE text-001.
PARAMETERS: p_r121 RADIOBUTTON GROUP g2,
            p_r122 RADIOBUTTON GROUP g2,
            p_r123 RADIOBUTTON GROUP g2,
            p_r124 RADIOBUTTON GROUP g2,
            p_r125 RADIOBUTTON GROUP g2.
SELECTION-SCREEN END OF BLOCK b2.
SELECTION-SCREEN END OF SCREEN 300.
```

```
SELECTION-SCREEN BEGIN OF SCREEN 400 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b3 WITH FRAME TITLE text-001.
PARAMETERS: p_r131 RADIOBUTTON GROUP g3,
            p_r132 RADIOBUTTON GROUP g3,
            p_r133 RADIOBUTTON GROUP g3,
            p_r134 RADIOBUTTON GROUP g3,
            p_r135 RADIOBUTTON GROUP g3.
SELECTION-SCREEN END OF BLOCK b3.
SELECTION-SCREEN END OF SCREEN 400.

* BLOQUE 2 *
SELECTION-SCREEN BEGIN OF SCREEN 500 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b4 WITH FRAME TITLE text-001.
PARAMETERS: p_r211 RADIOBUTTON GROUP g4,
            p_r212 RADIOBUTTON GROUP g4,
            p_r213 RADIOBUTTON GROUP g4,
            p_r214 RADIOBUTTON GROUP g4,
            p_r215 RADIOBUTTON GROUP g4.
SELECTION-SCREEN END OF BLOCK b4.
SELECTION-SCREEN END OF SCREEN 500.

* BLOQUE 3 *
SELECTION-SCREEN BEGIN OF SCREEN 600 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b5 WITH FRAME TITLE text-001.
PARAMETERS: p_r311 RADIOBUTTON GROUP g5,
            p_r312 RADIOBUTTON GROUP g5,
            p_r313 RADIOBUTTON GROUP g5,
            p_r314 RADIOBUTTON GROUP g5,
            p_r315 RADIOBUTTON GROUP g5.
SELECTION-SCREEN END OF BLOCK b5.
SELECTION-SCREEN END OF SCREEN 600.

* BLOQUE 4 *
SELECTION-SCREEN BEGIN OF SCREEN 700 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b6 WITH FRAME TITLE text-001.
PARAMETERS: p_r411 RADIOBUTTON GROUP g6,
            p_r412 RADIOBUTTON GROUP g6,
            p_r413 RADIOBUTTON GROUP g6,
            p_r414 RADIOBUTTON GROUP g6,
            p_r415 RADIOBUTTON GROUP g6.
SELECTION-SCREEN END OF BLOCK b6.
SELECTION-SCREEN END OF SCREEN 700.

SELECTION-SCREEN BEGIN OF SCREEN 800 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b7 WITH FRAME TITLE text-001.
PARAMETERS: p_r421 RADIOBUTTON GROUP g7,
            p_r422 RADIOBUTTON GROUP g7,
            p_r423 RADIOBUTTON GROUP g7,
            p_r424 RADIOBUTTON GROUP g7,
            p_r425 RADIOBUTTON GROUP g7.
SELECTION-SCREEN END OF BLOCK b7.
SELECTION-SCREEN END OF SCREEN 800.

SELECTION-SCREEN BEGIN OF SCREEN 900 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b8 WITH FRAME TITLE text-001.
PARAMETERS: p_r431 RADIOBUTTON GROUP g8,
            p_r432 RADIOBUTTON GROUP g8,
            p_r433 RADIOBUTTON GROUP g8,
            p_r434 RADIOBUTTON GROUP g8,
            p_r435 RADIOBUTTON GROUP g8.
SELECTION-SCREEN END OF BLOCK b8.
```

```
SELECTION-SCREEN END OF SCREEN 900.

SELECTION-SCREEN BEGIN OF SCREEN 210 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b9 WITH FRAME TITLE text-001.
PARAMETERS: p_r441 RADIOBUTTON GROUP g9,
            p_r442 RADIOBUTTON GROUP g9,
            p_r443 RADIOBUTTON GROUP g9,
            p_r444 RADIOBUTTON GROUP g9,
            p_r445 RADIOBUTTON GROUP g9.
SELECTION-SCREEN END OF BLOCK b9.
SELECTION-SCREEN END OF SCREEN 210.

* BLOQUE 5 *
SELECTION-SCREEN BEGIN OF SCREEN 310 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b10 WITH FRAME TITLE text-001.
PARAMETERS: p_r511 RADIOBUTTON GROUP g10,
            p_r512 RADIOBUTTON GROUP g10,
            p_r513 RADIOBUTTON GROUP g10,
            p_r514 RADIOBUTTON GROUP g10,
            p_r515 RADIOBUTTON GROUP g10.
SELECTION-SCREEN END OF BLOCK b10.
SELECTION-SCREEN END OF SCREEN 310.

SELECTION-SCREEN BEGIN OF SCREEN 410 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b11 WITH FRAME TITLE text-001.
PARAMETERS: p_r521 RADIOBUTTON GROUP g11,
            p_r522 RADIOBUTTON GROUP g11,
            p_r523 RADIOBUTTON GROUP g11,
            p_r524 RADIOBUTTON GROUP g11,
            p_r525 RADIOBUTTON GROUP g11.
SELECTION-SCREEN END OF BLOCK b11.
SELECTION-SCREEN END OF SCREEN 410.

* BLOQUE 6 *
SELECTION-SCREEN BEGIN OF SCREEN 510 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b12 WITH FRAME TITLE text-001.
PARAMETERS: p_r611 RADIOBUTTON GROUP g12,
            p_r612 RADIOBUTTON GROUP g12,
            p_r613 RADIOBUTTON GROUP g12,
            p_r614 RADIOBUTTON GROUP g12,
            p_r615 RADIOBUTTON GROUP g12.
SELECTION-SCREEN END OF BLOCK b12.
SELECTION-SCREEN END OF SCREEN 510.

SELECTION-SCREEN BEGIN OF SCREEN 610 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b13 WITH FRAME TITLE text-001.
PARAMETERS: p_r621 RADIOBUTTON GROUP g13,
            p_r622 RADIOBUTTON GROUP g13,
            p_r623 RADIOBUTTON GROUP g13,
            p_r624 RADIOBUTTON GROUP g13,
            p_r625 RADIOBUTTON GROUP g13.
SELECTION-SCREEN END OF BLOCK b13.
SELECTION-SCREEN END OF SCREEN 610.

* BLOQUE 7 *
SELECTION-SCREEN BEGIN OF SCREEN 710 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b14 WITH FRAME TITLE text-001.
PARAMETERS: p_r711 RADIOBUTTON GROUP g14,
            p_r712 RADIOBUTTON GROUP g14,
            p_r713 RADIOBUTTON GROUP g14,
            p_r714 RADIOBUTTON GROUP g14,
```

```
            p_r715 RADIOBUTTON GROUP g14.
SELECTION-SCREEN END OF BLOCK b14.
SELECTION-SCREEN END OF SCREEN 710.

SELECTION-SCREEN BEGIN OF SCREEN 810 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b15 WITH FRAME TITLE text-001.
PARAMETERS: p_r721 RADIOBUTTON GROUP g15,
            p_r722 RADIOBUTTON GROUP g15,
            p_r723 RADIOBUTTON GROUP g15,
            p_r724 RADIOBUTTON GROUP g15,
            p_r725 RADIOBUTTON GROUP g15.
SELECTION-SCREEN END OF BLOCK b15.
SELECTION-SCREEN END OF SCREEN 810.

* BLOQUE 8 *
SELECTION-SCREEN BEGIN OF SCREEN 910 AS SUBSCREEN .
SELECTION-SCREEN BEGIN OF BLOCK b16 WITH FRAME TITLE text-001.
PARAMETERS: p_r811 RADIOBUTTON GROUP g16,
            p_r812 RADIOBUTTON GROUP g16,
            p_r813 RADIOBUTTON GROUP g16,
            p_r814 RADIOBUTTON GROUP g16,
            p_r815 RADIOBUTTON GROUP g16.
SELECTION-SCREEN END OF BLOCK b16.
SELECTION-SCREEN END OF SCREEN 910.
```

INCLUDE ZCUESTIONARIO_TOP

```
*&---------------------------------------------------------------------*
*&  Include           ZCUESTIONARIO_TOP
*&---------------------------------------------------------------------*

*********************************************************************
*                    Variables
*********************************************************************
DATA: nrosubscreen(3)  TYPE n VALUE '200',
      nrosubscreen2(3) TYPE n VALUE '300',
      nrosubscreen3(3) TYPE n VALUE '400',
      nrosubscreen4(3) TYPE n VALUE '500',
      nrosubscreen5(3) TYPE n VALUE '600',
      nrosubscreen6(3) TYPE n VALUE '700',
      nrosubscreen7(3) TYPE n VALUE '800',
      nrosubscreen8(3) TYPE n VALUE '900',
      nrosubscreen9(3) TYPE n VALUE '210',
      nrosubscreen10(3) TYPE n VALUE '310',
      nrosubscreen11(3) TYPE n VALUE '410',
      nrosubscreen12(3) TYPE n VALUE '510',
      nrosubscreen13(3) TYPE n VALUE '610',
      nrosubscreen14(3) TYPE n VALUE '710',
      nrosubscreen15(3) TYPE n VALUE '810',
      nrosubscreen16(3) TYPE n VALUE '910',
      d_cont type i,
      d_total type i,
      v_resultado type char5.
```

DYNPRO 100

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0100.
 MODULE num_dympro.
 CALL SUBSCREEN AREA1 INCLUDING sy-repid nrosubscreen.
 CALL SUBSCREEN AREA2 INCLUDING sy-repid nrosubscreen2.
 CALL SUBSCREEN AREA3 INCLUDING sy-repid nrosubscreen3.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA1.
 CALL SUBSCREEN AREA2.
 CALL SUBSCREEN AREA3.
 MODULE USER_COMMAND_0100.
```

DYNPRO 110

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0110.
 MODULE num_dympro110.
 CALL SUBSCREEN AREA4 INCLUDING sy-repid nrosubscreen4.
 CALL SUBSCREEN AREA5 INCLUDING sy-repid nrosubscreen5.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA4.
 CALL SUBSCREEN AREA5.
 MODULE USER_COMMAND_0100.
```

DYNPRO 120

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0110.
 MODULE num_dympro120.
 CALL SUBSCREEN AREA6 INCLUDING sy-repid nrosubscreen6.
 CALL SUBSCREEN AREA7 INCLUDING sy-repid nrosubscreen7.
 CALL SUBSCREEN AREA8 INCLUDING sy-repid nrosubscreen8.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA6.
 CALL SUBSCREEN AREA7.
 CALL SUBSCREEN AREA8.
 MODULE USER_COMMAND_0100.
```

DYNPRO 130

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0110.
 MODULE num_dympro130.
 CALL SUBSCREEN AREA9 INCLUDING sy-repid nrosubscreen9.
```

```
 CALL SUBSCREEN AREA10 INCLUDING sy-repid nrosubscreen10.
 CALL SUBSCREEN AREA11 INCLUDING sy-repid nrosubscreen11.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA9.
 CALL SUBSCREEN AREA10.
 CALL SUBSCREEN AREA11.
 MODULE USER_COMMAND_0100.
```

DYNPRO 140

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0110.
 MODULE num_dympro140.
 CALL SUBSCREEN AREA12 INCLUDING sy-repid nrosubscreen12.
 CALL SUBSCREEN AREA13 INCLUDING sy-repid nrosubscreen13.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA12.
 CALL SUBSCREEN AREA13.
 MODULE USER_COMMAND_0100.
```

DYNPRO 150

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0110.
 MODULE num_dympro150.
 CALL SUBSCREEN AREA14 INCLUDING sy-repid nrosubscreen14.
 CALL SUBSCREEN AREA15 INCLUDING sy-repid nrosubscreen15.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA14.
 CALL SUBSCREEN AREA15.
 MODULE USER_COMMAND_0100.
```

DYNPRO 160

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0160.
 MODULE num_dympro160.
 CALL SUBSCREEN AREA16 INCLUDING sy-repid nrosubscreen16.

PROCESS AFTER INPUT.

 CALL SUBSCREEN AREA16.
 MODULE USER_COMMAND_0100.
```

DYNPRO 170

```
PROCESS BEFORE OUTPUT.
 MODULE STATUS_0170.
*
PROCESS AFTER INPUT.

 MODULE USER_COMMAND_0100.
```

El diseño gráfico de cada dynpro es muy similar por lo que sólo se muestra uno a modo de ejemplo.

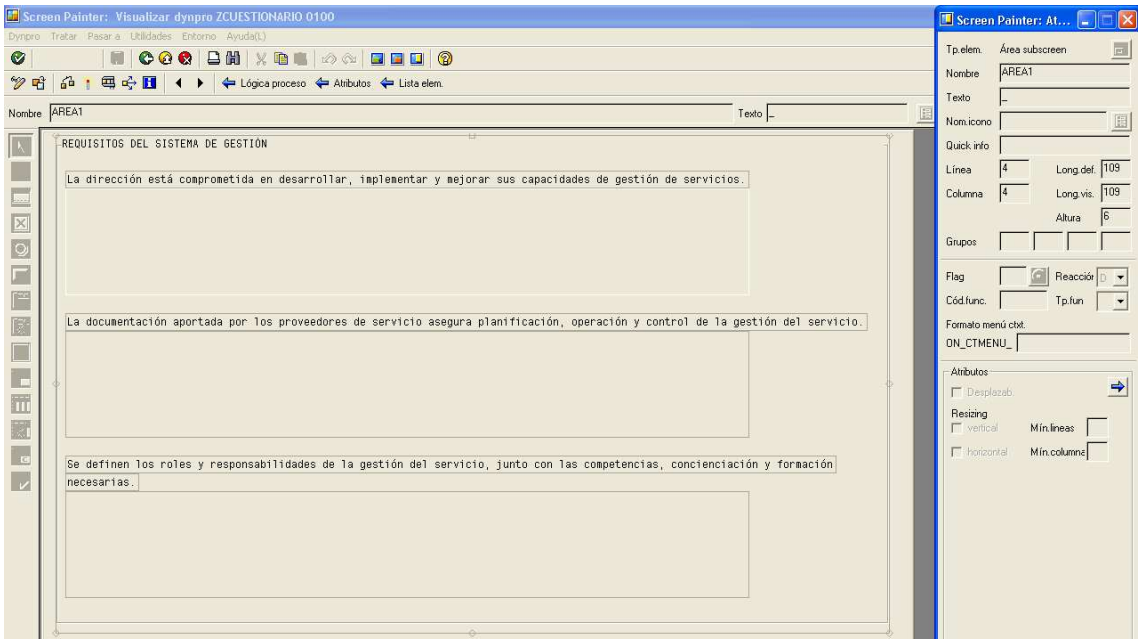


Imagen 26: Ejemplo diseño gráfico de una dynpro.

GLOSARIO

GLOSARIO

Acción Correctora: Proceso formal y sistemático de implantación de las mejoras. Su resultado es un cambio que mejora la calidad de salida de una determinada operación.

Acción Preventiva: Acción tomada sobre cualquier tipo de proceso destinada a eliminar una o varias causas conocidas de problemas, previniendo su aparición.

Actividad: Conjunto de tareas necesarias para obtener un resultado o producto.

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenazas: Cualquier acción o evento que puede ocasionar consecuencias adversas. Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Análisis de impacto al negocio: evaluar los resultados y las consecuencias de la inestabilidad.

Arquitectura: El diseño de la estructura y las relaciones de sus elementos.

Aseguramiento de la Calidad: Filosofía sobre la calidad que recoge el conjunto de las acciones, planificadas y sistemáticas, que son necesarias para proporcionar la confianza adecuada de que un bien o servicio va a satisfacer los requisitos dados sobre la Calidad.

El Aseguramiento de la Calidad no es complemento si los requisitos dados no reflejan íntegramente las necesidades del usuario.

Desde el punto de vista de la eficacia, el Aseguramiento de la Calidad implica, generalmente, una evaluación permanente de aquellos factores que influyen en la adecuación del proyecto y de las especificaciones a las aplicaciones previstas y, además, la verificación y la auditoría de las operaciones de la producción, de instalación y de inspección.

Ataques: Tipos y naturaleza de inestabilidad en la seguridad. Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Atributos de Calidad: "Componentes" del producto o servicio que el cliente es capaz de percibir con claridad y de forma diferenciada.

Auditabilidad: Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditado: Organización que se audita.

Auditor (Calidad): Persona calificada para realizar auditorías de calidad.

Auditor líder (calidad): Persona calificada para manejar y realizar auditorías de calidad.

Auditoría: Examen metódico e independiente realizado para determinar si las actividades y los resultados relativos al desarrollo de uno de los sistemas de la entidad satisfacen las disposiciones previamente establecidas, y para comprobar que estas disposiciones se llevan realmente a cabo y que son adecuadas para alcanzar los objetivos previstos.

Auditoría de Calidad: Examen metódico e independiente realizado para determinar si las actividades y los resultados relativos a la Calidad satisfacen las disposiciones previamente establecidas, y para comprobar que estas disposiciones se

llevan realmente a cabo y que son adecuadas para alcanzar los objetivos previstos.

La Auditoría de la Calidad se aplica especialmente, pero no se limita, a un sistema de la calidad o a alguno de sus elementos, a los procesos, a los productos o a los servicios. Tales auditorías se denominan, habitualmente, Auditorías del Sistema de la Calidad, Auditoría de la Calidad del Proceso, Auditoría de la Calidad de un producto, Auditoría de la Calidad del Servicio.

Uno de los objetivos de una Auditoría de Calidad es evaluar si es necesario introducir acciones de mejora y correctoras. No se debe confundir la Auditoría con actividades de supervisión o de inspección. El objetivo de éstas últimas es el control de un proceso o la aceptación de un producto.

Las Auditorías de la Calidad pueden realizarse por necesidades de orden interno o de orden externo.

Auditoría de los Planes de la Calidad: Auditoría que analiza las prácticas especificas referentes a la calidad y a los recursos y a las actividades aplicables a un determinado proceso, servicio, contrato o proyecto, recogidos en los Planes de la Calidad.

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Autocontrol: En su aceptación común, consiste en pasar al operario la responsabilidad de controlar la calidad de su trabajo. En Calidad Total significa responsabilizar al operario de la satisfacción de su cliente interno a través del control y mejora del proceso que se desarrolla en su puesto de trabajo.

Autorización: Lo que se permite cuando se ha otorgado acceso.

Calidad: Satisfacción de necesidades y expectativas razonables de los clientes a un precio igual o inferior al que ellos asignan al producto o servicio en función del "valor" que han recibido y percibido.

Calidad Concertada: Es el acuerdo establecido entre el comprador y el proveedor, según el cual, se atribuye al proveedor una determinada responsabilidad sobre la calidad de los lotes suministrados, que deben satisfacer unos niveles de calidad previamente convenidos. Este acuerdo conviene firmarlo en forma de contrato.

Calidad de Servicio: Desfase existente entre las necesidades y expectativas del cliente y su percepción del servicio recibido. Está muy condicionada por el "valor percibido" como única realidad a considerar.

Calidad Total: Filosofía sobre la Calidad que recoge el conjunto de las acciones planificadas y sistemáticas que son necesarias para conseguir la satisfacción del cliente.

En los años 70 aparece en Japón la expresión Company Wide Quality Control (CWQC). Significa Administración de la Calidad a lo Largo y Ancho de la Empresa, abarcando a todos y a cada uno de los miembros de la misma.

En Occidente se conoce como Calidad Total.

En los años 80, en Japón, el concepto de Gestión de la Calidad se amplia y adopta la denominación de Group Wide Quality Control (GWQC). Significa la Administración de la Calidad a lo Largo y Ancho del Grupo (expresión más amplia que empresa). Esto significa que la filosofía de la Calidad Total debe alcanzar a todos los miembros implicados.

Certificación: Acta en la que se da fe documental del cumplimiento de todos los requisitos exigidos.

Los requisitos pueden referirse al personal, al proceso, al producto, a las

organizaciones o a los servicios.

La certificación es una actividad en la cual el aseguramiento o garantía de la Calidad incide sobre la reglamentación, la aprobación y los requisitos que debe satisfacer un fabricante para cumplir con sus obligaciones legales. Es un medio mediante el cual un productor puede demostrar que cumple con estos requisitos.

Certificación del Sistema de la Calidad: Reconocimiento otorgado a un sistema de aseguramiento o garantía de la calidad, que ha demostrado que cumple todos los requisitos especificados en las normas aplicables.

"Cero defectos": Sistema experto para detectar los defectos tan pronto como se producen. Normalmente se utiliza para indicar un objetivo de perfección.

Círculo de Calidad: Grupo de personas de la misma sección que de forma voluntaria trabajan detectando problemas en su área y proponen soluciones para mejorar la Calidad.

Clasificación de datos: El proceso de determinar la sensibilidad y Criticidad de la información.

Cliente: Receptor de un producto aportado por el vendedor.

Comité de Calidad: Órgano de máxima jerarquía de la entidad que coordina, impulsa, planifica, asigna recursos y supervisa los Planes y Programas de la Calidad.

Componente organizativo: Llamado puesto de trabajo, departamento, sección, división, dirección,… Es una agregación lógica de tareas relativamente homogéneas, que se establecen por niveles según su amplitud. Suele tener denominaciones diferentes en las empresas como, por ejemplo, División, Dirección o Gerencia. El componente organizativo asume la responsabilidad de llevar a cabo las tareas y, para ello, recibe una autoridad delegada.

Conformidad: Cumplimiento de un elemento, proceso o servicio, de los requisitos de la especificación correspondiente.

La conformidad puede establecerse bien respecto a una sola característica, durante las fases de control o evaluación, o bien a todo el conjunto de los requisitos establecidos por la especificación.

Contra medidas: Cualquier acción o proceso que reduce la vulnerabilidad.

Control: En general y dentro del contexto de Gestión de la Calidad Total, el término control consiste en la "actividad de asegurarse que las acciones a tomar conducirán al resultado esperado". Se trata de controlar a priori los medios, en oposición al control tradicional a posteriori de los resultados. Otra acepción del término control, como una actividad dentro del proceso de gestión, consiste en recoger información para detectar desviaciones respecto de los objetivos fijados y poder así tomar buenas decisiones de mejora.

Control de Acceso: Limitar el acceso autorizado sólo a entidades autenticadas.

Control de Calidad: Técnicas y actividades de carácter operativo utilizadas para satisfacer los requisitos relativos a la calidad (UNE 66-001).

La función del control de calidad existe primordialmente como una organización de servicio, para interpretar las especificaciones establecidas por la ingeniería del producto y proporcionar asistencia al departamento de fabricación, para que la producción alcance estas especificaciones. Como tal, la función consiste en la colección y análisis de grandes cantidades de datos que después se presentan a diferentes departamentos para iniciar una acción correctiva adecuada.

Para comprender bien cada función es necesario conocer el concepto de calidad, la calidad del producto es en muchos aspectos, una característica intangible. La calidad la establece esencialmente el cliente, y se procura que el diseño y la

fabricación del producto para la venta, satisfaga estos requerimientos.

Controles: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

Costes de Calidad: Son aquellos en que la Empresa decide incurrir para conseguir la Calidad especificada. Se clasifican en costes de prevención, evaluación y fallos, internos y externos.

Costes asociados a la mala Calidad: Son todos los resultantes de actividades que no añaden "valor" para el cliente.

Criterio de Auditoría: Políticas, practicas, procedimientos o requerimientos contra los que el auditor compara la información recopilada sobre la gestión de calidad. Los requerimientos pueden incluir estándares, normas, requerimientos organizacionales específicos, y requerimientos legislativos o regulados.

Criticidad: La importancia que tiene un recurso para el negocio.

Defecto: Incumplimiento de un requerimiento relacionado con un uso previsto o especificado.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de ordenadores necesarias para la operación normal de un negocio.

Disponibilidad: Capacidad de un componente o servicio para realizar la función requerida en un instante o a lo largo de un período de tiempo determinado.

Disrupción: Una tecnología disruptiva es aquella que es capaz de robar un mercado entero por sí sola, las compañías clásicas son muy buenas a la hora de crear versiones mejoradas de productos ya existentes y su metodología es la siguiente: escuchar a los consumidores, invertir fuertemente en tecnologías que le den a los consumidores lo que buscan, altos márgenes económicos, tienen como objetivo principal a mercados más grandes en vez de otros más pequeños. Un producto disruptivo en cambio es visto inicialmente como inferior y ofrecen peor rendimiento que el resto de productos pero que llevan una serie de valores que son interesantes para el consumidor, al final con el tiempo estos productos van consiguiendo un mercado por sí solos hasta que crecen lo suficiente como para reemplazar a anteriores productos y convertirse en nuevos estándares industriales.

Eficacia: Se entiende como la cualidad que permite alcanzar los objetivos fijados, siendo su máximo exponente el contenido de la estrategia corporativa. Dando por supuesto que el principal objetivo de una Empresa que decide gestionar la Calidad Total es la satisfacción de sus clientes, diremos que algo es eficaz si permite con cierta seguridad alcanzar este objetivo.

Efectividad: Es la combinación de eficacia y eficiencia.

Eficacia: Medida de hasta qué punto se llevan a cabo las actividades planificadas y se alcanzan los resultados previstos.

Eficiencia: Es más un concepto económico y se refiere a la cantidad de recursos consumidos por unidad de producto aceptable. Los desperdicios y costos de la mala Calidad serían lo contrario de la eficiencia.

Equipo Auditor: Grupo de auditores, o un auditor individual, designados para desempeñar una auditoría dada; el equipo auditor puede incluir expertos técnicos y auditores en prácticas. Uno de los auditores del equipo de la auditoría desempeña la función de auditor líder.

Elemento de soporte lógico: Cualquier parte identificable del producto de soporte lógico en una etapa intermedia o en la etapa final del desarrollo.

Especificación de Calidad: Conjunto de requisitos que tiene que cumplir el producto o servicio para satisfacer los requisitos del cliente.

Estándar de Calidad: Conjunto de condiciones, expresadas por el cliente, que configuran la Calidad de aspectos concretos de un producto o servicio. Sirven de guía para la planificación y mejora de la Calidad. Cuantificación o concreción de los atributos.

Estrategia: Decisión que marca la línea de acción, a largo plazo, más adecuada para optimizar los resultados y que comporta la definición de los medios y de los recursos necesarios. Pasos que se requieren para alcanzar un objetivo.

Evaluación de la calidad: La evaluación de la calidad comprende aquellas actividades realizadas por una empresa, institución u organización en general, para conocer la calidad en ésta. Supervisa las actividades del control de calidad. A veces se define como "el control del control de calidad". Habitualmente se utilizan modelos de Calidad o referenciales, que permiten estandarizar el proceso de la evaluación y sus resultados, y por ello comparar. Los modelos de Calidad más conocidos en el mundo son el Deming, Malcom Baldrige, EFQM, etc. En ocasiones hay modelos sectoriales o locales, como en España el modelo Ciudadanía, propio del sector público.

Evidencia de Auditoría: Información, registros o declaraciones de hecho verificables. La evidencia de auditoría puede ser cualitativa o cuantitativa, es utilizada por el auditor para determinar cuando se cumple con el criterio de auditoría. La evidencia de auditoría se basa típicamente en entrevistas, revisión de documentos, observación de actividades y condiciones, resultados de mediciones y pruebas.

Experto técnico: Persona que provee el conocimiento y la experiencia especifica al equipo auditor, pero que no participa como un auditor.

Exposiciones: Áreas que son vulnerables a un impacto por parte de una amenaza.

Factor: En el diseño de experimentos, causa asignable que puede afectar a los resultados del ensayo y de la que se incluyen diferentes niveles de experimento.

Filosofía de la Calidad: Principios básicos con la relación a la calidad, y que condicionan las actividades que van a ser desarrolladas en un Sistema de la Calidad.

Función: Conjunto de todas las tareas relativas a un área, sin importar donde se realizan y quien las lleva a cabo.

Función Calidad: Conjunto de todas las tareas relativas a la calidad, sin considerar dónde se realizan y quién las lleva a cabo.

Garantía de la Calidad: Sinónimo de Aseguramiento de la Calidad.

Gerencia: Vigilar las actividades para garantizar que se alcancen los objetivos.

Gestión de la Calidad: Aspecto de la función general de la gestión que determina y aplica la Política de la Calidad.

La Gestión de la Calidad incluye: la planificación estratégica, la asignación de los recursos y otras actividades sistemáticas, tales como la planificación, las operaciones, las evaluaciones, relativas a la Calidad.

Gestión de servicio: Gestión de los servicios para cumplir con los requisitos de negocio.

Gobierno: Proporcionar control y dirección a las actividades.

Identificación: verificación de una persona o cosa; reconocimiento.

Impacto: Los resultados y consecuencias de que se materialice un riesgo. Medir la consecuencia al materializarse una amenaza.

Indicador de Calidad: Valor que permite juzgar el grado de cumplimiento de un estándar de Calidad.

Ingeniería de Calidad: Actividad de ingeniería que se ocupa de los principios y prácticas del aseguramiento del Control de la Calidad.

Dirige la planificación y el análisis de la calidad, específicamente para la prevención de defectos.

Inspección: acción de medir, examinar, ensayar o verificar una o varias características y de compararlas con los requisitos especificados con el fin de establecer su conformidad.

ISO 9000: Serie de normas internacionales por las que se rige el Aseguramiento de la Calidad, con un enfoque hacia el control de los procesos.

KSLOC: En miles de líneas de código. Es una medida tradicional de programa de lo grande que un programa es o cuánto tiempo o cuántas personas que se necesita para desarrollar un programa concreto. El código de medida suele ser el código fuente. Defectos por Kloc es una medida común utilizada como un objetivo o para evaluar la calidad del código.

Mantenibilidad: La medida en que el software puede ser mantenido.

Mantenimiento adaptativo: Permite la utilización de un producto software cuando se produce un cambio en su entorno.

Mantenimiento correctivo: Realizado específicamente para solucionar fallos existentes.

Mantenimiento de mejora: Para mejorar las prestaciones, la mantenibilidad u otros atributos del software.

Métricas de Seguridad, Monitoreo: Medición de actividades de seguridad.

Nivel: Grado alcanzado por cualquier característica. En el diseño de experimentos, los niveles de un factor son los valores o modalidades del factor que se está examinando.

Nivel de Calidad: Cualquier medida relativa de la calidad obtenida por comparación entre los valores observados y los requeridos.

Normalmente se expresa mediante un valor numérico, denominado valor de calidad, que indica el grado de conformidad o disconformidad, con los requisitos establecidos.

No repudio: no se puede negar un evento o una transacción.

Norma: Patrón de referencia, fijado previamente, que garantiza la uniformidad de un sistema, proceso, bien o servicio.

Normas: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Norma de calidad: Una norma de calidad es un documento, establecido por consenso y probado por un organismo reconocido (nacional o internacional), que proporciona, para un uso común y repetido, reglas, directrices o características para las actividades de calidad o sus resultados, con el fin de conseguir un grado óptimo de orden en el contexto de la calidad. Los principales organizaciones internacionales, emisoras de normas de calidad son: ISO (Organización Internacional de Estándares) y IEC (Comisión Electrónica Internacional).

Objetivo: Punto que se pretende alcanzar o conseguir como resultado de una operación.

Pharming: explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que

haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

Phishing: Término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas .

Dado el creciente número de denuncias de incidentes relacionados con el *phishing* se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, campañas para prevenir a los usuarios y con la aplicación de medidas técnicas a los programas.

Plan: Documento que recoge las formas de operar, los recursos y la secuencia de actividades ligadas a la consecución de unos objetivos.

Plan de Calidad: Adaptación del Sistema de Calidad a la producción de un determinado producto o contrato.

Políticas: Declaración de alto nivel sobre la intención y la dirección de la gerencia.

Política corporativa de Calidad: Declaración escrita que compromete a todos los integrantes de la Empresa con la consecución, y mejora en su caso, de la Calidad.

Procedimiento: Recopilación del objetivo, alcance, responsabilidades y forma de realizar determinadas actividades de la gestión en la entidad. Puede estar documentada por escrito o ser una práctica historia no documentada.

Proceso: Sistema de actividades que usan recursos para transformar entradas en salidas (las entradas pueden ser salidas de otros procesos).

Proceso de la Calidad Total: Es también sinónimo de la Calidad Total. Con la palabra proceso, se quiere dar a entender que la Cálida Total como meta es una utopía. La Calidad Total en si es un proceso o un estado permanente de Mejora (Mejora continua y sin límites).

Proceso de Mejora Continua de la Calidad: Conjunto de enfoques, de actividades y de acciones que hay que llevar a cabo para integrar, en el proceso de dirección, los conceptos y las prácticas de la mejora de la calidad.

Programa: Conjunto documentado de actividades, recursos y accione que sirven para la implantación y desarrollo de cualquier sistema que exista en la entidad.

Programa de la Calidad: Conjunto documentado de actividades, recursos y acciones que sirve para la implantación de un sistema de calidad en la organización.

Proyecto: Proceso único que consta de un conjunto de actividades coordinadas y controladas, con fechas de inicio y de fin, y orientadas a alcanzar un objetivo de acuerdo con requerimientos específicos, incluyendo restricciones de tiempo, de coste y de recursos.

Registro: Documento que recoge los resultados alcanzados o que aporta evidencia de las actividades realizadas.

Registro de Calidad: Documento que presenta la información oportuna para demostrar el grado de cumplimiento con la Calidad requerida.

Resultados de la Auditoría: Resultados de la evaluación de la evidencia de auditoría recopilada comparada contra los criterios de auditoría acordados. Los resultados de la auditoría proveen la base para el reporte de la auditoría.

Revisión: Actividad realizada para asegurar la idoneidad, adecuación, eficacia y eficiencia de algo que ha de alcanzar los objetivos establecidos.

Riesgo: La explotación de una vulnerabilidad por parte de una amenaza. Posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.

Riesgo residual: El riesgo que permanece después de que se han implementado contra medidas y controles.

Seguridad en capas: La defensa a profundidad que contenga la inestabilidad.

Sensibilidad: El nivel de impacto que tendría una divulgación no autorizada.

Servicio: Producto intangible que es el resultado de al menos una actividad, realizada en la interfaz entre el proveedor y el cliente.

Servicio de Calidad: Aquel que iguala o supera las expectativas del cliente.

Sistema: El sistema equivale a la Función más el conjunto de procedimientos que ligan a unas tareas con otras. El sistema de la Calidad, el sistema Comercial, son dos ejemplos.

Sistema de Calidad: Conjunto de responsabilidades, procedimientos procesos y recursos de la estructura de la organización que se establecen para gestionar la Calidad (ISO-8402).

Sistema de gestión de la calidad: El sistema de gestión de la calidad es el conjunto de elementos interrelacionados de una empresa u organización por los cuales se administra de forma planificada la calidad de la misma, en la búsqueda de la satisfacción de sus clientes. Entre dichos elementos, los principales son: la estructura de la organización, sus procesos, sus documentos y sus recursos.

El sistema de gestión de la calidad en una organización tiene como punto de apoyo el manual de calidad, y se completa con una serie de documentos adicionales como manuales, procedimientos, instrucciones técnicas, registros y sistemas de información. Normalmente existe un responsable de calidad que velará por el cumplimiento de lo dispuesto. Normalmente sigue una norma de calidad.

SLOC: Líneas de código fuente. Se utiliza para medir el tamaño de un programa, contando el número de líneas del programa fuente. SLOC se suele utilizar para predecir la cantidad de esfuerzo que se requiere para desarrollar un programa, así como para estimar la productividad de programación, el esfuerzo una vez que se produce el software o la calidad del código.

Soporte Lógico: Creación intelectual que comprende los programas, procedimientos, reglas y cualquier documentación asociada a la operación de un sistema de procesos de datos.

Suministrador: Entidad que aporta un producto al cliente.

Uniformidad: La uniformidad permite el intercambio de partes, principio básico en la fabricación moderna. La uniformidad no implica identidad absoluta. La variación depende de los siguientes factores:

1. La variación permisible que no destruya la unidad del producto o la aceptación del consumidor.
2. La variación generada por las desviaciones inevitables en el funcionamiento de las máquinas en las que se hará el trabajo y de las personas que operan las máquinas.

La variación generada por las características del material que entra a la planta, tanto para procesarlo como para emplearlo en el proceso.

Validación (para soporte lógico): Es el proceso de evaluación del soporte lógico para asegurar el cumplimiento con los requisitos especificados.

Verificación: acción de revisar, inspeccionar, ensayar, comprobar, supervisar o cualquiera otra análoga, que establezca y documente que los elementos, procesos, servicio o documentos están conformes con los requisitos especificados.

Verificación (soporte lógico): Es el proceso de evaluación de los productos de una fase dada para asegurar la corrección y consistencia respecto a los productos y normas proporcionadas como entradas a esta fase.

Vulnerabilidades: Deficiencias que pueden ser explotadas por amenazas.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

- Normas ISO/UNE proporcionadas por la Universidad Carlos III.
- Jan Van Bon, Marianne Nugteren, Selma Polter
  ISO/IEC 20000 Guía de bolsillo
  Van Haren Publishing
- Camison Zornoza, César
  Gestión de la calidad: Conceptos, enfoques, modelos y sistemas
  Pearson Educación, 2006.
- Ullman, Larry E.
  PHP, guía de aprendizaje.
  Pearson Educación, D.L. 2004
- Sangüesa, Marta
  Teoría y práctica de la calidad.
  Thomsom Editores Spain, 2006
- Páginas web:
  www.es.sgs.com
  www.webtaller.com
  www.php.net
  www.forosdelweb.com
  www.emagister.com
  www.monografias.com
  www.gestiopolis.com
  www.inei.gob.pe
  www.ali.es
  www.wikilearning.com
  www.angelfire.com
  www.mouse.cl
  www.lapetiteclaudine.com
  www.cibersocsiedad.net
  www.error500.net
  www.filmica.com
  www.abadiadigital.com
  www.elpais.es
  www.merodeando.com
  www.enter.es
  www.vsantivirus.com

www.iso27000.es

spanish.jabatonet.com

barrapunto.com

news.bbc.co.uk

eprints.rclis.org

es.wikipedia.org

descargas.abcdatos.com

iso20000enespanol.com

javascripts.astalaweb.com

seguinfo.blogspot.com

tecniart.net

elastico.net

sociedaddelainformacion.telefonica.es