1. INTRODUCCIÓN

La Auditoría Informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, y que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas.

En la presente unidad trataremos los aspectos vinculados a la revisión de los sistemas informáticos y de Tecnologías de Información y la Comunicación (TICs), de una forma conceptual.

Además, y de forma práctica, se ofrecerán una serie de herramientas, elaboradas por **ISACA** (del inglés, *Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)*), como organismo internacional reconocido, que publica herramientas y estándares de auditoría y control de sistemas de información.

Estas herramientas se ofrecen al alumno como una base de actuación a un posible análisis preliminar, con una doble misión:

- Poder identificar el "grado de complejidad las TICs". Se trata de dotar, al compliance Officer o responsables de supervisión, de una herramienta que le ayude a identificar el tamaño y complejidad del entorno informático de una organización en concreto.
- Poder realizar, para organizaciones de una complejidad baja, un "checking" de controles generales. Es decir, una evaluación, sobre los principales aspectos, para poder obtener una confianza razonable en la seguridad del sistema.

Estos controles, a su vez, se aplicarán en tres dominios:

- Seguridad Lógica y Física.
- Proceso de desarrollo de aplicaciones, adquisiciones y nuevos desarrollos
- Explotación de sistemas.

El conocimiento de esta herramienta basada en dar un apoyo para la revisión de entornos informatizados, proporciona:

- Conocimiento del control interno de la organización al órgano de control del sistema de cumplimiento legal.
- Incrementa la formación técnica de las personas que ocuparan tarea vinculadas con el Corporate compliance, en un entorno informatizado.
- Dota al personal relacionado con el Corporate compliance de una guía de evaluación de los entornos informatizados, basada en la Norma Técnica de Auditoría de Cuentas en Entornos Informatizados.

Para analizar sistemas de mayor complejidad, será necesario poder contar con el trabajo de expertos en el campo de la seguridad y el entorno informático.

2. DETERMIANCIÓN DEL GRADO DE COMPLEJIDAD DE LAS TI EN LA ORGANIZACIÓN.

El total de elementos de las TI constituyen un entramado complejo de conceptos, técnicas, productos, dispositivos y sistemas. Por tanto, su evaluación de forma global, para que no sea arbitraria, tiene que basarse en un modelo conceptual a la vez amplio y estructurado.

Estructuras de TI complejas exigirán de un trabajo posterior de revisión y verificación por profesionales altamente cualificados y con conocimientos técnicos muy específicos en el área informática. Estructuras menos complejas podrán ser examinadas por profesionales que, si bien estén familiarizados con los principales aspectos de revisión informática, no necesitarán de un conocimiento técnico tan profundo.

En este apartado se intenta atender al trabajo preliminar de poder identificar ese grado de complejidad, mediante un cuestionario de 24 preguntas. Permite al profesional revisor evaluar el grado de complejidad TI de esa organización y, por tanto, determinar si es necesario disponer de conocimientos especializados, y en qué medida.

2.1. GRADO DE COMPLEJIDAD. PRINCIPALES ASPECTOS.

Una vez definido el objetivo, pasamos a definir los principales aspectos y conceptos tenidos en cuenta para el test:

2.1.1. Indicadores de Estructura (Hardware):

La palabra "hardware" en informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Podemos decir que son los elementos de la estructura informática físicia de la organización.

2.1.1.1. Servidores:

En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

En este sentido, y para nuestro análisis, el concepto de servidor a tener en cuenta será el segundo. Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

- En Internet, un servidor es un ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras.
- En redes locales se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos.
- Los Servidores almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML.

En nuestro test, la determinación del número de servidores que tenga la organización será uno de los elementos identificativos de su complejidad. De este modo, se han otorgado las siguientes ponderaciones para su evaluación:

- Si nº servidores <2; Valor 0.
- Si nº servidores <2 >=4; Valor 2.
- Si nº servidores >4; Valor 5.

2.1.1.2. Sistemas Operativos:

Este apartado mide el grado de complejidad en relación a si el sistema operativo que utiliza la organización es un sistema estándar, o, por el contrario, no lo son o utiliza varios sistemas.

Así mismo, para estructuras más complejas, se considera el uso de sistemas Múltiples o WAN, sigla de Wide Area Network ("Red de Área Amplia"). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de red WAN es la propia Internet.

¿Utiliza Windows Server?

"*Windows Server*" es una marca que abarca una línea de productos del servidor de Microsoft Corporation y consiste en un sistema operativo diseñado para servidores de Microsoft y una gama de tipos de productos dirigidos al mercado más amplio de

negocios; Windows Server incluye, por ejemplo, interfaz de usuario, el administrador de tareas, el IP address management, entre otros. Podríamos considerar que es el sistema estándar por antonomasia. Es un sistema muy extendido, sobre todo a nivel usuario, hogares y pequeñas y medianas empresas, sin grandes complejidades. Es, por este motivo, por el que esta pregunta se considera un indicio de la complejidad de las TI en la organización. El que se opere con este sistema indicará, por lo general, una baja complejidad.

Se han otorgado las siguientes ponderaciones para su evaluación:

- Sí; Valor 0.
- No; Valor 3.

2.1.1.3. Estaciones de trabajo.

En informática una estación de trabajo (en inglés *Workstation*) es un computador de altas prestaciones destinado para trabajo técnico o científico. En este sentido, cuantas más estaciones existan en la organización, podemos considerar que esta será más compleja. Así, se ha considerado para su evaluación:

- Entre 1 y 6; Valor 0.
- Entre 7 y 16; Valor 2.
- Más de 16; Valor 5.

2.1.2. Indicadores de la propia organización.

El tamaño y su organización a nivel informático será otro indicativo del nivel de complejidad de la entidad. La existencia de un propio departamento informático, o la existencia de esta función de forma externalizado, número de personas dedicadas, así como los recursos, número de centros de tratamiento de datos… serán indicativos de indicio para medir la complejidad:

2.1.2.1. Departamento interno de TI:

El hecho de que la empresa tenga constituido un departamento específico para TI, con atribuciones propias es un indicativo bastante apropiado para poder determinar aspectos sobre la complejidad. En el test, este hecho se evalúa de la siguiente forma:

- Sí; Valor 5.
- No; Valor 0.

2.1.2.2. Número de personas del Departamento interno de TI:

Además del hecho de que exista o no este departamento, también habrá que evaluar el tamaño del mismo, en función del personal asignado por la organización. En el test, los valores aportados han sido

- Si no existe departamento propio de IT; Valor 0.
- Entre 1 y 2 personas; Valor 2.
- Más de 2 personas; Valor 5.

2.1.2.3. Número de centros de tratamientos de datos:

Además de la central, el número de localizaciones remotas que originen datos en la organización, serán indicadores de la complejidad. Así, por ejemplo, si existen distintas delegaciones que realizan independientemente el tratamiento contable, que luego es consolidado (centros de costes independientes), serán un hecho que aporte mayor complejidad.

En el test, los valores aportados han sido:

- Si sólo hay 1 centro; Valor 0.
- Si hay 2 centros; Valor 2.
- Más de 2 centros; Valor 5.

2.1.3. Indicadores relacionados con las Aplicaciones (Softwares).

Una aplicación informática se puede definir como una **solución informática para la automatización de ciertas tareas complicadas**, como pueden ser la contabilidad, la redacción de documentos, o la gestión de un almacén. Algunos ejemplos de programas de aplicación son:

- procesadores de textos
- hojas de cálculo
- base de datos
- de comunicación de datos
- multimedia
- para presentaciones
- de diseño gráfico,
- de cálculo
- de finanzas y contabilidad
- correo electrónico
- navegador web
- compresión de archivos
- presupuestos de obras
- gestión de empresas
- gestión documental
- etc.

Ciertas aplicaciones desarrolladas "a medida" suelen ofrecer una gran potencia ya que están exclusivamente diseñadas para resolver un problema específico (ejemplo, Navision, SAP, u otros ERPs). Otros, llamados paquetes integrados de software, ofrecen menos potencia, pero a cambio incluyen varias aplicaciones, como un programa procesador de textos, de hoja de cálculo y de base de datos (ejemplo, Microsoft Office).

Actualmente, con el uso de dispositivo móviles se ha extendido el término app, aplicación informática para dispositivos móviles o tabletas con multitud de funcionalidades. Desde juegos hasta aplicaciones para realizar tareas cotidianas. Es un abanico enorme que hacen más interactivo los dispositivos móviles.

2.1.3.1. Aplicaciones de negocios utilizadas (Softwares- ERP):

Una vez vista la definición de aplicación, la cuestión será estudiar cuál o cuáles son las aplicaciones de negocio utilizadas por la organización.

La gran importancia de las nuevas tecnologías de la información y su creciente presencia en los diversos ámbitos de la empresa moderna, conlleva cada vez más la presencia de programas informáticos aplicados a la gestión empresarial de las organizaciones.

El software de gestión empresarial es un tipo de programa diseñado para soportar un segmento de la empresa. Casi todas las funciones comunes de una organización (bases de datos de clientes, nóminas, contabilidad, etc).

Los ERP son una solución robusta para aquellas empresas que buscan una solución universal a la centralización de su información. El ERP es un sistema integral de gestión empresarial que está diseñado para modelar y automatizar la mayoría de procesos en la empresa (área de finanzas, comercial, logística, producción, etc.). Su misión es facilitar la planificación de todos los recursos de la empresa.

"ERP" son las siglas en inglés de Enterprise Resource Planning. En español, Planificación de Recursos Empresariales. Actualmente, un ERP puede funcionar prácticamente en cualquier empresa moderna. Todas las actividades de todos los sectores de una empresa involucrados en la actividad con los clientes, pueden ser gestionadas a través de un ERP.

A continuación, se ofrecen algunos nombres de los principales ERPs del mercado:

- **NAVISION**
- **SAP**
- **ORACLE**
- **SAGE X3, XRT, MURANO**
- FOUR SHIFT
- BAAN
- WORKMETER
- SAIN

Una aplicación básica y muy extendida a nivel contable y de gestión para pequeñas entidades, es Contaplus, por tanto, el hecho de que esta aplicación sea la principalmente utilizada por la entidad para sus registros contables, sin estar integrada en ninguna otra herramienta, será un indicativo del tamaño poco complejo, en el área informática, de la entidad. Sin embargo, la utilización de otras aplicaciones ERPs, serán indicativo de mayor complejidad:

- Contaplus o similares; Valor 0.
- Navision o similares; Valor 2.
- SAP o similares; Valor 5.

- ***Cuadro 1:*** *Cuadro de complejidad de aplicaciones.*

Básica	Media	Alta
sage ContaPlus	NAVISION software	SAP R/3
contasol	sage X3	
a3ASESOR con	SAP Business One	ORACLE PEOPLESOFT
NCS SOFTWARE	Sage Murano ERP	

2.1.3.2. Aplicaciones adaptadas a la empresa:

La mayoría de las compañías de software permiten realizar una serie de "adaptaciones" a sus paquetes básicos de aplicaciones. De este modo, y contratando servicios de consultoría informática y asistencia técnica muchos de los operadores permiten adaptación "ad hoc", conforma a las necesidades de las organizaciones.

El hecho de que se hayan producido adaptaciones a estas aplicaciones, es otro indicativo de un mayor grado de complejidad:

- Sí; Valor 3.
- No; Valor 0.

2.1.3.3. Integración de las aplicaciones entre sí (interface o interfaz):

En informática, se utiliza para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles permitiendo el intercambio de información. Su plural es interfaces.

Si hablamos de software, las interfaces físicas son las relaciones producidas entre dos aplicaciones para el uso de datos. Así, por ejemplo, la información suministrada por una aplicación propia usada por la maquinaria de la fábrica puede ser enviada a la aplicación de gestión, con el fin de medir la productividad, unidades, y cualquier otro factor, de una forma automática.

Para que estas interfaces puedan funcionar correctamente, es necesario que tenga un "lenguaje compatible". Son importantes los "sistemas de gestión de bases de datos" para estas operaciones.

A la pregunta ¿están integradas las distintas aplicaciones? Los valores asignados han sido:

- Sí; Valor 2.
- No; Valor 0.

2.1.3.4. Frecuencia de modificaciones en las aplicaciones de negocio.

La realización de modificaciones frecuentes en las aplicaciones de gestión y de negocio es otro indicador de complejidad. Cuantas más modificaciones se produzcan, significará que la entidad es más "activa" en términos informáticos, a la vez de más compleja.

A esta cuestión, las valoraciones aportadas han sido:

- Sí; Valor 5.
- No; Valor 0.

2.1.3.5. ¿Los informes y reportes (legales, por ejemplo, informes financieros), son los estándares de la aplicación?

Otro indicador de la complejidad y dedicación aplicada al desarrollo y complejidad informática puede obtenerse al verificar sui la organización emite los reportes financieros (u otros requeridos), utilizando los modelos de informes estándares ofrecidos por la propia aplicación, o, por el contrario, si ha programado desarrollos a medida con las especificaciones dadas expresamente, de forma que se obtengan informes adaptados.

A esta cuestión, las valoraciones aportadas han sido (preguntas 10, 11 y 12 del cuestionario "*2-PT grado complejidad de TI.xls*"):

a) Preguntar si los informes son los estándares de las aplicaciones (no hay desarrollos especiales:

- Sí; Valor 0.
- No; Valor 1.

b) Si la respuesta anterior es "No", especificar si, además de los informes estándares usados, algunos son a medida:

- Sí; Valor 1.
- No; Valor 0.

c) Si la respuesta anterior es "No", especificar si, la gran mayoría de los informes son a medida:

- Sí; Valor 2.
- No; Valor 0.

2.1.3.6. ¿Se utilizan aplicaciones adicionales a los informes aportados por la aplicación (por ejemplo, Excel)?

Si, con el fin de poder completar la información a aportar en un informe o reporte, la organización tiene que hacer uso de varias aplicaciones adicionales a la aplicación de gestión principal, es un indicio de un mayor nivel de complejidad en las necesidades estructurales y, por ende, informáticas, de la entidad.

A esta cuestión, las valoraciones aportadas han sido:

- Sí; Valor 3.
- No; Valor 0.

2.1.4. Indicadores relacionados con la complejidad del sistema.

Además de los procesos de interrelación de la organización consigo misma (ya hemos fisto las redes, servidores, interfaces entre aplicaciones…), pueden existir procesos más complejos dirigidos a obtener datos de agentes externos a la organización (clientes, proveedores…). Albaranes, facturas, órdenes de compra y otros documentos comerciales electrónicos pueden tramitarse directamente desde la computadora de la empresa emisora a la de la empresa receptora, con gran ahorro de tiempo y evitando muchos errores, propios de la comunicación tradicional «en papel».

Si bien, la existencia de estos sistemas, suponen un ahorro y ventaja para las organizaciones, que, a su vez, necesitan de una alta complejidad y estructura informática para poder funcionar adecuadamente.

Así mismo la realización de comercio electrónico es otra de las operaciones que exigen un grado de complejidad mayor.

2.1.4.1. Intercambio electrónico de datos" (en inglés Electronic Data Interchange o EDI).

Es el intercambio electrónico de datos estructurados vía formato de mensajes estandarizados desde una aplicación a otra con una intervención manual mínima. Un sistema EDI envía los datos desde un sistema interno al sistema de un socio comercial en unos segundos.

Cada día grandes cantidades de documentos, como Pedidos, Facturas, Artículos del Catálogo, Datos del Mercado, etc. son insertados manualmente y usando métodos tradicionales (Correo, Fax, e-mail). Estos métodos tradicionales de comunicación (creación manual, impresión, ensobre, envío postal y captura manual del receptor) ofrece gran potencial de mejoras. De esta forma tan clásica, la información pasa por muchas fases y personas en su trayecto en la organización. Además, cuanto menos automatizado es el proceso de intercambio, es más arriesgado y propenso a errores.

Este intercambio puede realizarse en distintos formatos: EDIFACT, XML, ANSI ASC X12, TXT, etc.

El proceso:

a) El mensaje

Para que los socios operen vía EDI, es necesario un acuerdo sobre el estándar del mensaje. Los principales estándares para este lenguaje son:

- EDIFACT
- VDA
- ANSI X.12
- ODETTE
- XML
- GALIA
- EANCOM
- RosettaNet
- SWIFT
- ebXML
- ELEMICA
- TRADACOMS

b) El Software EDI

Está compuesto de conectores y un conversor. El conversor es el corazón del software EDI que traduce los datos (mensajes) desde un formato interno de la empresa a un estándar EDI y viceversa. Los principales Partners/Sistemas ERP que permiten EDI son:

- SAP
- QAD
- ORACLE
- Baan
- Navision
- IFS
- abas
- Brain
- Intentia
- inform
- J.D.Edwards

c) La comunicación

Después de que los datos (mensaje) han sido traducidos del formato interno al formato estándar por el software EDI, necesita ser enviado al destinatario deseado. Son necesarios canales de comunicación como, por ejemplo: Redes de Valor Añadido (Value Added Networks (VAN)), ISDN, X.25, conexión analógica punto a punto, intranet y la mayoría de las extranet de mercados específicas como ANX/ENX (la extranet de la industria de automoción).

A esta cuestión, las valoraciones aportadas han sido (preguntas 14, y 14.1 del cuestionario "*2-PT grado complejidad de TI.xls*"):

a) Preguntar si existen proceso EDI:

- Sí; Valor 3.
- No; Valor 0.

b) Si la respuesta anterior es "Sí", especificar con cuantos terceros se produce el intercambio electrónico de datos:

- Si la respuesta anterior ha sido "No"; Valor 0.
- Hasta 1; Valor 0.
- Entre 1 y 2; Valor 1.
- Entre 3 y 5; Valor 2.
- A partir de 6. Valor 5.

2.1.4.2. Comercio Electrónico automatizado con clientes.

Consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Hoy en día, se refiere, principalmente, a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

La cantidad de comercio llevada a cabo electrónicamente ha crecido de manera extraordinaria debido a Internet. Una gran variedad de comercio se realiza de esta manera, estimulando la creación y utilización de innovaciones como la transferencia de fondos electrónica, la administración de cadenas de suministro, el marketing en Internet, el procesamiento de transacciones en línea (OLTP), el intercambio electrónico de datos (EDI), los sistemas de administración del inventario y los sistemas automatizados de recolección de datos.

A esta cuestión, las valoraciones aportadas han sido (preguntas 15, 15.1, 15.2 y 15.3 del cuestionario "*2-PT grado complejidad de TI.xls*"):

1. Preguntar si se realiza comercio electrónico automatizado con clientes:

- Sí; Valor 3.
- No; Valor 0.

2. Si la respuesta anterior es "Sí", especificar el grado de automatización de estas operaciones:

- Si la respuesta anterior ha sido "No"; Valor 0.
- Parcialmente; Valor 5.
- Totalmente; Valor 2.

3. Considerar la importancia de las operaciones de comercio electrónico en relación al total volumen de facturación de la organización:

- Inferior al 1% Valor 0.
- Entre el 1% y el 5%; Valor 3.
- Superior al 5%; Valor 5

4. Considerar la importancia de las operaciones de comercio electrónico en relación al total volumen de operaciones de la organización:

- Inferior al 5% Valor 0.
- Entre el 5% y el 25%; Valor 2.
- Superior al 25%; Valor 3.

2.1.5. Externalización del servicio de TICs.

Consiste en contar con la asistencia de entidades externas especializadas, para prestar gestión, total o parcial, asesoramiento, servicios y materiales, relacionados con el campo de la informática.

La externalización del servicio de soporte TI tiene una serie de ventajas asociadas como el ahorro de costes. Las empresas proveedoras de servicios TI incluyen en sus paquetes de productos soporte informático realizado por profesionales especializados que pueden ayudar en la capacitación y adopción de la nueva solución TI a los empleados, así como realizar reparaciones o labores de mantenimiento o incluso ayudar al propio Responsable Informático de la empresa –si lo hubiese- en dichas labores de gestión de software y hardware. Se evita que la empresa invierta tiempo en dichas tareas y así podrá centrarse en las ventas. El ahorro económico y de tiempo es evidente.

2.1.5.1. Externalización en la gestión de aplicaciones.

Se analiza si la organización tiene externalizada la función de implantación y gestión (instalación, actualización, licencias…) sobre los softwares de uso en la misma.

A esta cuestión, las valoraciones aportadas han sido:

- Sí; Valor 3.
- No; Valor 0.

2.1.5.2. Externalización en la gestión de estructuras.

Se analiza si la organización tiene externalizada la función de implantación y gestión (instalación, actualización, licencias…) sobre las estructuras técnicas en la misma.

Las funciones atribuibles al departamento de informática son muchas y han ido cambiando con los años. Hoy en día, podríamos hablar de las siguientes, en materia de estructura, entre otras:

- Gestión del correo electrónico, la red privada de usuarios y el sistema de mensajería instantánea.
- Gestión de la red telefónica de la compañía.
- Mantenimiento y gestión de los servicios de Internet.
- Administración y mantenimiento del sitio web corporativo
- Soporte de usuarios para actualizaciones o reparaciones de servicios informáticos.
- Instalación y actualización de hardware.
- Recuperación de datos y gestión de bases de datos.
- Formación de empleados.
- Revisión y actualización de los criterios de seguridad.

A esta cuestión, las valoraciones aportadas han sido:

- Sí; Valor 2.
- No; Valor 0.

2.1.6. Juicio profesional del auditor

Finalmente, y como última cuestión al análisis, se incluye una cuestión basada únicamente en el juicio subjetivo profesional del auditor del sistema informático, con el fin de que haga una valoración sobre la percepción que tiene de la complejidad del sistema informático de la entidad.

A esta cuestión, las valoraciones aportadas han sido:

- Bajo; Valor 1.
- Medio; Valor 4.
- Alto; Valor 7.

3. CONTROLES GENERALES DE SISTEMAS DE INFORMACIÓN.

En un mundo que depende cada día más de los servicios proporcionados por los soportes informáticos, es vital definir procedimientos en caso de un posible fallo o siniestro. Cuando ocurra una contingencia, es esencial que se conozca el detalle, el motivo que la originó y el daño causado, lo que permitirá recuperar, en el menor tiempo posible, el proceso perdido. También se debe analizar el impacto futuro en la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las TICs, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitirán analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En el presente apartado, se pretende dar al lector una guía básica de comprobación, con el fin de poder analizar, **sólo en el caso en los que se determine que el entorno de TI es de una complejidad baja**, por sí mismo, una serie de controles generales, que le permitan evaluar la solvencia de la organización en el campo de TI.

Dicha **Guía ha sido elaborada por ISACA (Barcelona Chapter)**, como consecuencia de los requerimientos que para el sector de la auditoría financiera son requeridos a los auditores de cuentas. Dicho modelo es exportable al campo del Corporate Compliance, de forma que el responsable de control de cumplimiento legal pueda hacer uso de esta herramienta. No obstante, esta guía no deberá tenerse en cuenta como un único "check list" ni visión única, sino que deberán tenerse en cuenta los conceptos que se definen en la presente unidad formativa, además de complementos de formación en materia de TICs que el usuario deberá adquirir.

De forma esquemática, los controles se han dividido en tres familias principales:

- **Controles de Seguridad Lógica y Física (SL).** Para evitar accesos no deseados o no autorizados, así como para salvaguardar la integridad física de los recursos.
- **Controles de Proceso y Desarrollo (PD).** Relacionados con la evolución de las aplicaciones, compatibilidades y nuevas aplicaciones.
- **Controles de Explotación de Sistemas (MS).** Relacionados con la seguridad en la salvaguarda de copias de información y salvaguarda de datos

A continuación, se ofrece un estudio pormenorizado de los mismos:

3.1. CONTROLES DE SEGURIDAD LÓGICA Y FÍSICA (SL).

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma.

Hay dos aspectos que siempre se deben tener en cuenta en cualquier trabajo de revisión o auditoría:

- **Riesgo:** Es todo tipo de debilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las organizaciones.

- **Seguridad:** Es una forma de protección contra los riesgos.

Así mismo, en referencia la seguridad en el entorno TI, la podemos dividir:

- **Seguridad lógica**: Es la configuración adecuada del sistema para evitar el acceso a los recursos y configuración del mismo por parte de personas no autorizadas, ya sea a nivel local o vía red. Mucha gente considera que seguridad es solamente la seguridad lógica, pero este concepto es erróneo.

- **Seguridad física:** Cuando se quiere tener un equipo seguro es importante considerar todos los aspectos que están involucrados. Uno de ellos y sin duda, uno de los más importantes, es la seguridad que ofrece el entorno donde está ubicado el equipo.

A continuación, pasamos a enumerar y describir brevemente los principales aspectos a verificar en este sentido:

SL.1. Política de seguridad.

Consiste en comprobar **si se dispone de una política de seguridad de la información, aprobada por la Dirección**, comunicada a todo el personal de la organización.

La política de seguridad es un documento, explícitamente aprobado por la dirección, donde ésta se compromete a implantar y supervisar una serie de controles en materia de seguridad de la información.

Es un documento breve que contiene una declaración de intenciones genérica acerca de los aspectos más relevantes para la dirección, como por ejemplo la regulación del uso de los recursos de la organización únicamente para el desempeño de las funciones del empleado, o la obligación de reportar a la dirección cualquier incidente de seguridad.

En consecuencia, se debe preguntar por la existencia de una política de seguridad y si ésta se encuentra aprobada por la dirección y ha sido debidamente actualizada.

En caso de que se disponga de ella, se adjuntará como evidencia del control. En caso contrario, es posible que la organización disponga de algún procedimiento de más bajo nivel, como por ejemplo "política de gestión de usuarios" o "política de respaldo". Se solicitará evidencia de todos los documentos relacionados con estos aspectos disponibles.

Ver SL1.PDF

SL.2. Identificación de Usuarios.

Consiste en comprobar **si la Organización ha establecido un mecanismo de identificación/autenticación** para los sistemas de información, que proporcione responsabilidad individual (cuentas individuales por usuario).

Preguntar al responsable del proceso de creación de usuarios si se dispone de alguna regla sobre nomenclatura de usuarios o normativa al respecto, como por ejemplo que todos los usuarios comiencen por la inicial del nombre y el primer apellido de la persona (julian perez = jperez)

Preguntar si hay excepciones a esta regla. Como ejemplos de excepciones, podrían ser las siguientes:

- **Usuarios administradores del sistema,** suelen utilizar usuarios "admin" o similar.
- **Usuarios de fábrica o de producción,** que suelen compartir el mismo usuario en función de su turno de fabricación.
- **Usuarios de recepción,** que suelen compartir también en función de su turno de trabajo.

Adjuntar como evidencia cualquier normativa formalizada al respecto.

Ver SL2.PDF

SL.3. Política de contraseñas.

Consiste en comprobar **si la organización ha definido controles de autenticación basados en la existencia de contraseñas**. La política de seguridad contiene las reglas de administración y sintaxis de las mismas.

Preguntar al administrador por la política corporativa de contraseñas. Se encuentre formalizada o no, dicha política debería contener al menos los siguientes aspectos:

- **Caducidad** (cada cuánto tiempo el usuario debe cambiar la contraseña)
- **Bloqueo por intentos fallidos** (número de intentos de gracia que el usuario dispone hasta el bloqueo de la cuenta).
- **Complejidad** (Requisitos de complejidad como usar minúsculas y mayúsculas, usar signos de puntuación o no usar nombres de diccionario)
- **Tiempo de inactividad** (tiempo de inactividad en el sistema, tras el cual el usuario queda bloqueado y se debe reintroducir la contraseña)
- **Longitud mínima y máxima de la contraseña.**
- **Histórico de contraseñas** (al cambiar de contraseña, el usuario no puede volver a repetir un número determinado de contraseñas antiguas)

Ver SL3.PDF

SL.4. Autorización de usuarios.

Consiste en comprobar si **los usuarios disponen de permisos en el sistema de acuerdo a las funciones que desempeñan**. Dichos permisos se encuentran aprobados por sus responsables y cumplen una adecuada segregación de funciones.

No disponer de controles sobre la asignación de permisos sobre los usuarios puede conllevar que personal interno acceda, modifique o elimine información para la que no tiene autorización.

Preguntar al responsable de sistemas por la "política de accesos" a los sistemas. La política de accesos es la que define a qué puede acceder y a qué no un usuario de la organización.

La política de accesos de la organización debería cumplir los siguientes requisitos:

- **Todos los accesos deben ser autorizados por el responsable de la información accedida.** Es decir, el responsable del área de contabilidad (o sus jerárquicamente superiores) debería ser el que decidiera quién puede acceder y quién no a la información sobre contabilidad.
- **El usuario tendrá acceso únicamente a la información que necesita para el desempeño de sus funciones.** Por ejemplo, un usuario de contabilidad no

debería tener acceso a la aplicación de RRHH a menos que también realice funciones de formación o gestión de personal.

- **Se deben cumplir requisitos de segregación de funciones.** Por ejemplo, siempre que sea posible, evitar que el mismo usuario que realice un pedido sea el mismo que realice el pago de dicho pedido.

Ver SL4.PDF

SL.5. Gestión de usuarios.

Consiste en comprobar la Organización ha implementado controles para **garantizar que las altas, bajas y modificaciones de usuarios se gestionan de manera oportuna** para reducir el riesgo de accesos no autorizados o inapropiados

No disponer de una adecuada gestión de usuarios puede conllevar accesos no autorizados a los sistemas, realizados incluso por personal no perteneciente a la organización (creación de usuarios no autorizados) o por usuarios dados de baja en la organización.

Preguntar al responsable de sistemas por el procedimiento de gestión de usuarios. Un procedimiento de gestión de usuarios describe los pasos a seguir cuando se da de alta un usuario en el sistema, cuando se da de baja y cuando un usuario es trasladado de posición.

Para cualquiera de los procesos descritos (alta, baja o modificación de usuarios), es fundamental que el procedimiento contenga la necesidad de una petición, por parte del responsable autorizado. Esta petición debería contener:

- **En el caso de las altas,** el detalle del nuevo usuario y los permisos de acceso concretos que se le deben facilitar. Cuando sea necesario deberá incluir los equipos que necesita (ordenadores, móviles, tarjetas de acceso, etc.).

- **En el caso de las modificaciones,** el detalle de los nuevos permisos de accesos y cualquier otra variación necesaria en el equipo físicos.

- **En el caso de las bajas,** el detalle del usuario a dar de baja y la fecha a partir de la cual no deberá disponer de acceso. En este caso también se debería incluir un procedimiento para gestionar la información pendiente (por ejemplo, redireccionar todo el correo recibido al responsable jerárquico durante un tiempo)

Ver SL5.PDF

SL.6. Usuarios administradores.

Comprobar que **los usuarios con mayores privilegios de acceso en el sistema son utilizados únicamente por personal autorizado y de forma segura**.

Se trata de evitar el Riesgo asociado sobre accesos no autorizados a la información de la organización, con el agravante de que los usuarios avanzados pueden realizar acciones más críticas que los usuarios normales (como por ejemplo crear usuarios falsos en el sistema, modificar la seguridad del sistema para no ser descubiertos, etc.)

Preguntar al responsable de **sistemas si se han definido políticas específicas para los usuarios administradores del sistema.**

Estas políticas deberían contemplar un cumplimiento estricto de las medidas recomendadas en los controles SL2, SL3, SL4 y SL5. Por ejemplo, en el control SL3 se recomienda que las contraseñas de los usuarios se deban modificar periódicamente, siendo adecuado un cambio cada 45 o 60 días. En el caso de los usuarios administradores se debería recomendar que se modificaran cada 45 días como máximo.

Por otra parte, los sistemas suelen venir con un usuario "administrador" por defecto. Este usuario administrador es el que se utiliza en el momento de la instalación y posee una contraseña también "por defecto". Por ejemplo, en Windows se dispone del usuario "administrator", cuya contraseña siempre es la misma. En este sentido, las políticas deben recomendar que no existan usuarios administradores con contraseñas por defecto.

Ver SL6.PDF

SL.7. Seguridad física.

Comprobar que **La Organización ha implementado controles que garanticen la protección física de los servidores y equipos críticos.**

La Organización debería disponer de medidas de protección física de los equipos críticos y servidores, puesto que su inexistencia podría afectar a la disponibilidad de la información (como por ejemplo un incendio o una inundación) o su confidencialidad (accesos no autorizados).

Preguntar al responsable de sistemas por los procedimientos que establecen las medidas de protección física para el CPD (centro de procesado de datos) y los centros de comunicaciones.

Las medidas de protección física para el CPD pueden ser de dos tipos:

- **Ambientales:** El CPD debería disponer de mecanismos de refrigeración para no sobrecalentarse además de sistemas de detección de humos y extinción de incendios, entre otros.
- **De Acceso:** Al CPD solamente debería acceder personal autorizado, y en consecuencia debería encontrarse cerrado.
- **Consultar también si estas medidas físicas se revisan** adecuadamente para validar su adecuación (por ejemplo, los extintores deben ser revisados periódicamente)

Ver SL7.PDF

SL.8. Controles antivirus.

Comprobar que **la Organización dispone de programas de protección frente a códigos maliciosos (virus, troyanos, escaneo de información, etc.).**

En cuanto a Antivirus, la organización debe disponer de un procedimiento de adquisición y actualización periódica de la herramienta antivirus (entendiendo virus en sentido amplio, es decir, malware, spyware, spam, etc.).

Como prueba de diseño, se debe preguntar al responsable de sistemas de qué forma se supervisa esta función y si dispone de procedimientos escritos al respecto.

Las medidas a comprobar, denberán ir dirigidas a verificar la existenca de:

- **Antivirus de correos electrónicos.**
- **Antivirus de correos sistema.**

Ver SL8.PDF

SL.9. Supervisión de la seguridad.

Comprobar que la **Organización dispone de mecanismos de supervisión periódicos sobre los controles de seguridad**.

No disponer de una adecuada supervisión de la seguridad conlleva un empeoramiento progresivo de los controles de seguridad implantados.

El objetivo de este control es garantizar que los controles de seguridad son implementados y ejecutados por una persona pero supervisados periódicamente por una persona diferente.

Preguntar al responsable de **sistemas si se han definido políticas específicas para los usuarios administradores del sistema.**

Estas políticas deberían contemplar un cumplimiento estricto de las medidas recomendadas en los controles SL2, SL3, SL4 y SL5. Por ejemplo, en el control SL3 se recomienda que las contraseñas de los usuarios se deban modificar periódicamente, siendo adecuado un cambio cada 45 o 60 días. En el caso de los usuarios administradores se debería recomendar que se modificaran cada 45 días como máximo.

Por otra parte, los sistemas suelen venir con un usuario "administrador" por defecto. Este usuario administrador es el que se utiliza en el momento de la instalación y posee una contraseña también "por defecto". Por ejemplo, en Windows se dispone del usuario "administrator", cuya contraseña siempre es la misma. En este sentido, las políticas deben recomendar que no existan usuarios administradores con contraseñas por defecto.

Ver SL6.PDF

3.2. CONTROLES DEL ÁREA DE DESARROLLO (PD).

Permiten alcanzar la eficacia del sistema, economía, eficiencia, integridad de datos, protección de recursos y cumplimiento con las leyes y regulaciones a través de metodologías como la del Ciclo de Vida de Desarrollo de aplicaciones.

Es decir, son los controles que van dirigidos a la comprobación de las implantaciones de sistemas, y modificaciones que, a lo largo de la vida de la organización, se van produciendo sobre los mismos. Instalación de nuevas aplicaciones, sustituciones, modificaciones, ampliaciones, nuevas versiones…

A continuación, pasamos a enumerar y describir brevemente los principales aspectos a verificar en este sentido:

PD.1. Gestión de Cambios.

Comprobar si la Organización **ha establecido controles para garantizar que los cambios/desarrollos realizados sobre los sistemas son aprobados por los responsables del departamento al que va dirigido la modificación, una vez han sido probados.**

Se trata de evitar que se puedan realizar desarrollos no aprobados por los responsables adecuados, o no probados adecuadamente. Esto puede conllevar que la organización tenga en sus sistemas aplicaciones potencialmente peligrosas desde dos puntos de vista:

- **Aplicaciones fraudulentas,** como, por ejemplo, una aplicación que permita llevarse un céntimo de cada transacción contable a una cuenta específica de un usuario.
- **Aplicaciones erróneas**, como, por ejemplo, una aplicación que, aunque se haya ideado con la mejor intención, bloquea todo el sistema e impide realizar el cierre contable mensual**.**

En primer lugar, se debe preguntar si existe una metodología de desarrollo. Una metodología de desarrollo es un procedimiento específico del área de sistemas que describe y detalla el proceso a seguir cuando se desea modificar o mejorar las aplicaciones de la organización. Este proceso suele contener las siguientes fases:

- **Toma de requerimientos de usuario.**
- **Evaluación, priorización del proyecto, asignación de recursos y estudio de viabilidad.**
- **Análisis funcional y técnico.**
- **Pruebas a realizar (especialmente las pruebas de usuario)**
- **Procedimiento para poner la aplicación o cambio al alcance de todos los usuarios.**
- **Procedimiento de supervisión de que la aplicación o cambio funciona correctamente.**

Ver PD1.PDF

PD.2. Cambios autorizados.

Comprobar si **la Organización ha diseñado controles para garantizar que los cambios en el entorno real son realizados por personal autorizado.**

Se trata de evitar que se puedan realizar desarrollos no aprobados por los responsables adecuados, o no probados adecuadamente. Esto puede conllevar que la organización tenga en sus sistemas aplicaciones potencialmente peligrosas desde dos puntos de vista:

- **Aplicaciones fraudulentas,** como, por ejemplo, una aplicación que permita llevarse un céntimo de cada transacción contable a una cuenta específica de un usuario.
- **Aplicaciones erróneas**, como, por ejemplo, una aplicación que, aunque se haya ideado con la mejor intención, bloquea todo el sistema e impide realizar el cierre contable mensual**.**

Debería existir una "prueba de cambios en entrono real":

- **Preguntar si existe un procedimiento para cambios en un entorno real.**
- **Peguntar quien es el que se encarga, y si tiene autorización para ello.**
- **Preguntar si ese responsable es, a su vez, desarrollador, o se dedica únicamente al mantenimiento de los sistemas, y si dispone del suficiente conocimiento y experiencia sobre las aplicaciones de la organización.**

Ver PD2.PDF

PD.3. Adquisición de aplicaciones y servidores.

Comprobar si **la Organización ha implementado controles para garantizar que en las adquisiciones de aplicaciones y servidores se minimizan los riesgos relacionados con la factibilidad del proyecto y la integración con las aplicaciones e infraestructura actuales.**

Se trata de evitar que la organización adquiera aplicaciones o servidores inadecuados, poco fiables o directamente incompatibles con los sistemas actuales. Este aspecto puede conllevar desde gastos innecesarios a un funcionamiento deficiente del entorno informático.

Se debe disponer de una política (o procedimiento) de adquisición de aplicaciones y servidores.

Este procedimiento debe contener, al menos, los siguientes aspectos:

- **Se debe disponer de al menos tres opciones de adquisición,** correspondientes a distintos proveedores o soluciones. Las soluciones deben ser comparables entre sí mediante una serie de parámetros estándar, como por ejemplo, precio, características del proveedor o características del producto.

- **Las adquisiciones deben ser aprobadas por la dirección de la organización y también por la dirección del área de sistemas.**

- **Cada adquisición debe acompañarse de un plan de proyecto** que tenga en cuenta un plan de pruebas adecuado y un análisis de factibilidad.

Ver PD3.PDF

PD.4. Cambios de emergencia.

Comprobar si la **Organización ha implementado controles para garantizar que los cambios de emergencia se realizan de forma adecuada y controlada.**

Se trata de evitar errores en modificaciones sobre las aplicaciones existentes que no se encuentren aprobadas, supervisadas ni revisadas, y que se tenga que realizar por carácter de urgencia.

Este aspecto puede conllevar peligrosas desde dos puntos de vista:

- Aplicaciones fraudulentas, como, por ejemplo, una aplicación que permita llevarse un céntimo de cada transacción contable a una cuenta específica de un usuario.

- Aplicaciones erróneas, como, por ejemplo, una aplicación que, aunque se haya ideado con la mejor intención, bloquea todo el sistema e impide realizar el cierre contable mensual.

Este procedimiento debe contener, al menos, los siguientes aspectos:

- **Identificación de situaciones sobre las que aplicar el procedimiento de cambios de emergencia.**

- **Aprobación de la aplicación del procedimiento, usuarios especiales autorizados a realizar este tipo de cambios y trazabilidad de las acciones realizadas.**

- **Documentación posterior de los cambios realizados y revisiones posteriores.**

Ver PD4.PDF

PD.5. Integración nuevas aplicaciones.

Comprobar si la **Organización dispone de procedimientos para evaluar cómo afectan los nuevos desarrollos o la adquisición de paquetes de software que se realizan, al funcionamiento habitual de los sistemas de información, considerando el impacto en los procesos de negocio y la información generada.**

Se trata de evitar impactos inesperados sobre las aplicaciones de negocio que existen.

Evaluar si una nueva aplicación o desarrollo tendrá algún efecto inesperado antes de que ocurra, es complicado. Por este motivo muchas organizaciones no tienen este procedimiento formalizado y confían en la experiencia del personal responsable.

En este sentido, el auditor puede validar dos grandes aspectos:

- **La persona responsable de esta evaluación dispone de suficiente experiencia con las aplicaciones de la organización.** Este aspecto puede deducirse mediante una entrevista y también analizando información objetiva, como, por ejemplo, la experiencia del responsable en el puesto o puestos similares, número de incidencias producidas en aplicaciones estables, etc.

- **Las herramientas disponibles para la evaluación.** Los responsables de sistemas suelen disponer de diccionarios de datos o "mapas" de aplicaciones, que permiten analizar las interacciones entre las distintas aplicaciones de la organización. En el caso expuesto en este apartado, se podría ver en el "mapa" que la modificación del nuevo IVA utiliza una base de datos ya utilizada por el módulo de ventas, y que, por tanto, podría verse afectado.

Ver PD5.PDF

PD.6. Entorno de pruebas.

Comprobar si la **organización dispone de varios entornos de desarrollo y controles suficientes para garantizar que únicamente se aplican las modificaciones y actualizaciones que han sido debidamente probadas.**

Se trata de evitar que la organización realice las pruebas de una nueva aplicación o desarrollo en el mismo entorno en el que se encuentran los usuarios. Esto podría provocar errores graves en la información gestionada. (Por ejemplo, si alguien del área de sistemas está probando la modificación para actualizar el nuevo tipo de IVA en el entorno real, al mismo tiempo que un usuario de contabilidad está preparando las facturas del mes, es posible que se emita a un cliente una factura falsa, correspondiente a una "prueba", en lugar de la correcta.

Preguntar al responsable de sistemas por los entornos disponibles en la organización:

- **Entorno de desarrollo.** Es el entorno donde los programadores realizan su trabajo y prueban que lo que están modificando les funciona bien.
- **Entorno de integración.** Es un entorno de pruebas donde los desarrolladores prueban distintos módulos a la vez.
- **Entorno de pre-producción, o calidad.** Es un entorno, habitualmente una copia del entorno real, aunque falsa, donde se realizan las pruebas de usuario y globales.
- **Entorno real,** también denominado producción. Es el entorno conocido por todos los usuarios de la organización.
- **Preguntar también por los requisitos que debe tener un desarrollo para pasar de un entorno al siguiente**.
- **El auditor solicitará cualquier documento formalizado** (normativa o procedimiento) en este sentido como evidencia de auditoría.

Ver PD6.PDF

PD.7. Selección de proveedores.

Comprobar si la **Organización ha implementado controles para garantizar que la selección de los proveedores de servicios externos se realiza de acuerdo con la política de gestión de proveedores de la organización.**

Se trata de evitar la selección de proveedores de forma ineficiente, que pueda conllevar pérdidas para la organización. También se trata de evitar prácticas fraudulentas en la contratación en el seno de la organización.

Consultar si dicho procedimiento, formalizado o no, contiene los siguientes aspectos:

- **Selección de entre al menos, tres opciones de proveedores.** Los proveedores deben ser comparables entre sí mediante una serie de criterios cuantitativos (precio, servicios ofrecidos, antigüedad y solvencia en el sector) y cualitativos (experiencia de la organización con el proveedor, valor añadido).
- **Dos o más personas implicadas en el proceso de selección.**
- **Necesidad de aprobación de la selección por la dirección del área de sistemas y por la dirección de la organización.**

Ver PD7.PDF

PD.8. Acuerdos de Nivel de Servicio.

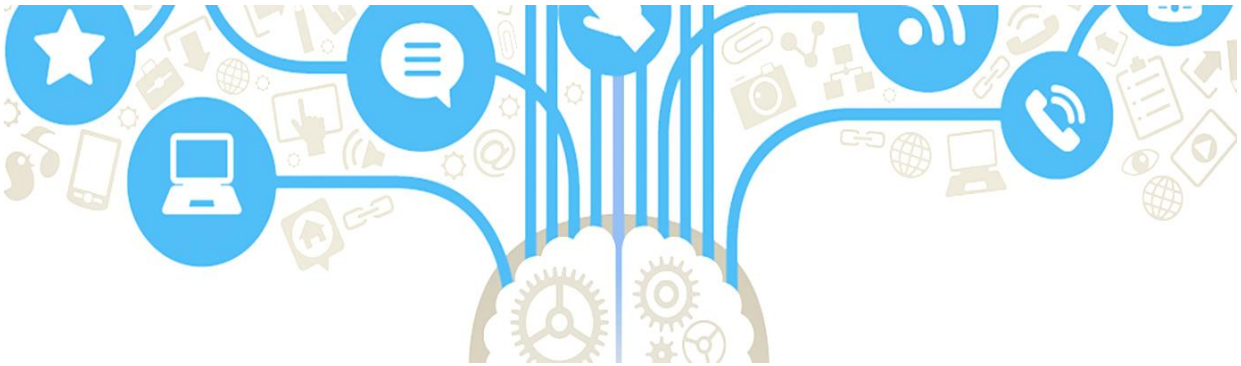
Comprobar si la **Organización ha contratado un proveedor teniendo en cuenta un nivel de servicio mínimo exigible adecuado a las necesidades de negocio.**

Se trata de evitar la selección de proveedores que no cumplan los requerimientos técnicos apropiados, y puedan originar problemas, una vez se haya iniciado la relación con los mismos (solvencia).

Consultar:

- **Si se dispone de contratos "estándar" en la organización** que contemplen aspectos relacionados con los acuerdos de niveles de servicio (ANS) con proveedores del área de sistemas.
- **En caso de no disponer de cláusulas específicas preparadas**, preguntar al responsable de sistemas **si dispone de un listado de "mínimos"** a cumplir por un proveedor en caso de contratación de un servicio.
- **Solicitar listado de todos los proveedores informáticos y sus contratos.**

Ver PD8.PDF



3.3. CONTROLES DEL ÁREA DE EXPLOTACIÓN (MS).

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.

Habitualmente, una de las áreas de sistemas se denomina explotación porque se encarga de que "siga funcionando todo lo que el usuario utiliza". Esto incluye herramientas ofimáticas, carpetas personales, correo electrónico, y por supuesto, las aplicaciones específicas, como de contabilidad o Recursos Humanos.

Cuantos más procesos automatizados tiene una organización, más relevante es esta función.

Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. aspectos relacionados, por tanto, con los datos, son, el tratamiento y realización de copias de seguridad, la supervisión de los procesos de sistemas, la gestión de incidencias, protección de hojas de cálculo u otras herramientas de tratamiento de datos…

A continuación, pasamos a enumerar y describir brevemente los principales aspectos a verificar en este sentido:

MS.1. Copias de Seguridad.

Comprobar si **la Organización ha implementado controles para garantizar la existencia y validez de copias de seguridad de los datos, configuraciones de bases de datos, configuraciones de sistemas operativos y aplicaciones.**
Se trata de evitar que, en caso de pérdida o deterioro de información, dicha pérdida sea definitiva y la información no pueda ser recuperada, como consecuencia de que no se han realizado políticas de copia de seguridad adecuadas.

En primer lugar, se debe preguntar si existe una **política de respaldo**. Esta suele contener la determinación sobre los siguientes puntos:

- **Periodicidad de las copias** (cada cuántos días, semanas, meses o años).
- **Tipo de las copias** (puede haber copias completas o incrementales).
- **Almacenamiento de las copias** (por ejemplo, en cintas, o en discos)
- **Retención de las copias** (cuánto tiempo se mantienen las copias diarias, semanales, mensuales o anuales)
- **Procedimiento de generación de copias de respaldo.**
- **Procedimiento de recuperación de información, en caso necesario.**

Ver MS1.PDF

MS.2. Pruebas periódicas de Copias de Seguridad.

Comprobar si **la Organización ha implementado controles para garantizar la existencia y validez de copias de seguridad de los datos, configuraciones de bases de datos, configuraciones de sistemas operativos y aplicaciones.**

Es muy parecido al objetivo del punto MS.1. Se trata de evitar que, en caso de pérdida o deterioro de información, dicha pérdida sea definitiva y la información no pueda ser recuperada, como consecuencia de que no se han realizado políticas de copia de seguridad adecuadas.

El impacto de este riesgo puede ser leve (perder información de un fichero concreto que se puede volver a generar) o en su extremo poner en riesgo la continuidad de la organización.

Se debe preguntar si existe:

- **Existencia de un Procedimiento de recuperación de la información.**
- La persona que solicita la recuperación, **debe contar con la debida autorización (manejo de datos sensibles).**
- **No sólo es importante la existencia del proceso, sino la realización del mismo.**
- Que en cada recuperación **quede constancia de la persona que la realizó, y la fecha.**
- **Tener un listado de todas las recuperaciones realizadas.**

Ver MS2.PDF

MS.3. Supervisión de los procesos de sistemas.

Comprobar si **la Organización ha implementado controles para garantizar que el entorno de producción es supervisado para identificar incidentes y fallos.**

No supervisar adecuadamente las aplicaciones y sistemas de la organización puede facilitar la generación de errores, derivando en un mal funcionamiento de los mismos.

Este mal funcionamiento puede afectar a la integridad (por ejemplo, modificando datos contables sin autorización), confidencialidad (por ejemplo, robo de información) y disponibilidad de la información (caída de los sistemas).

Se debe preguntar si:

- **Existencia de mecanismos para monitorizar el rendimiento de los equipos y de sus conexiones.**
- ¿Existe un **procedimiento escrito**?
- Comprobar las actualizaciones sobre las versiones de softwares.

Ver MS3.PDF

MS.4. Gestión de incidencias.

Comprobar si **la Organización ha implementado controles para garantizar que las incidencias de integridad de datos y de control de accesos son registradas, analizadas, resueltas oportunamente y reportadas a la Dirección.**

El objetivo es evitar una inadecuada gestión de las incidencias de integridad de datos, que podría provocar la existencia de información errónea en la organización. El impacto de esta información errónea puede ir desde pequeñas modificaciones al valor de adquisición de materia prima hasta una cuenta de resultados incorrecta. También podría provocar que información sensible sea accedida por personas no autorizadas, comprometiendo la confidencialidad de la información e incluso también su integridad.

Se debe preguntar si existe un procedimiento de detección y gestión de incidencias con, al menos, los siguientes puntos:

- **Mecanismos de detección.** Los sistemas deberían tener mecanismos automáticos de detección de incidencias. Por ejemplo, en integridad, validar que el importe pagado coincide con el importe de la factura emitida. En control de accesos, por ejemplo, que la misma persona no se encuentra conectada a la vez en dos ordenadores distintos.
- **Registro.** Toda incidencia debe quedar registrada y adecuadamente catalogada. En el registro debe constar toda la información posible que ayude a su resolución.
- **Asignación.** Toda incidencia debe tener un responsable claro asignado.
- **Priorización/Criticidad.** Las incidencias deben ser priorizadas de forma que los responsables de su resolución comiencen por las más críticas.
- **Gestión y resolución.** Se debe tener trazabilidad del tiempo que se ha tardado en su resolución, las acciones que se han tomado y cuándo queda cerrada.

- **Aprobación**. Todas las incidencias deben ser aprobadas por la persona que las ha generado, de forma que se haya comprobado que han sido correctamente resueltas.

- **Escalado.** En ocasiones, una incidencia puede exceder la capacidad de la persona asignada para su resolución. Se deben tener instrucciones claras de a quién elevar la incidencia en este tipo de casos.

- **Seguimiento.** Debe haber un responsable de realizar un seguimiento de las incidencias y comprobar que todas son atendidas de forma adecuada.

Ver MS4.PDF

MS.5. Protección de Hojas de Cálculo

Comprobar si **la Organización ha establecido controles sobre documentos de usuario importantes, como hojas de cálculo, que intervienen en la elaboración de la información financiera.**

En este aspecto, tres son los ámbitos principales de incidencias:

- **De Integridad** (Datos erróneos o inexactos)
- **De Confidencialidad** (Acceso a información por personal no autorizado)
- **De Disponibilidad** (Pérdida de información).

Se debe preguntar si:

- **Se guarda copia de seguridad de las hojas críticas.**

- Si existen medidas de protección lógica, como, por ejemplo, el requerimiento de contraseñas.

- Si se dispone de controles para verificar la coherencia de los cálculos y que éstos no hayan sido modificados.

Ver MS5.PDF

MS.6. Traspasos de información.

Comprobar si **los intercambios de información entre sistemas (manuales y automáticos) disponen de los controles oportunos de integridad.**

Se trata de evitar traspasos incorrectos de información, que puedan afectar a la elaboración de información y provocar errores de integridad en los estados o reportes a emitir (por ejemplo, estados financieros).

En términos de auditoría de sistemas se distinguen dos tipos de "volcados":

- **Automático**, es decir, no hay ninguna intervención manual. En el ejemplo anterior, el usuario puede apretar un botón en la aplicación de RRHH y automáticamente se vuelcan los pagos aprobados a la aplicación contable.

- **Manual,** donde hay intervención humana relevante. En el ejemplo anterior, el usuario realiza una consulta en la aplicación de RRHH donde extrae a Excel la información sobre los pagos y luego carga el Excel en la aplicación contable.

Se debe preguntar si:

- **Existencia de un responsable en los procesos de "volcado"**
- Si los volcados son **manuales o automáticos**.
- En los procesos **manuales, además de la existencia del responsable, debería existir un proceso de controles manuales.**

Ver MS6.PDF

MS.7. Ejecución de los procesos automáticos.

Comprobar si **La organización ha establecido controles para garantizar que los procedimientos automáticos cumplen con los requerimientos de la entidad y con las normativas que les afecta.**

En este caso, se verificará que el proceso se desarrolla y ejecuta de forma correcta y que los niveles de control establecidos por la entidad garantizan la corrección del proceso.

Se trata de evitar la ejecución de procesos automáticos no aprobados puede conllevar fraude interno o información errónea.

Cuantos más procesos automatizados tiene una organización, más relevante es este control.

Los procesos automáticos se planifican y suelen ejecutarse habitualmente por las noches o fines de semana, cuando los sistemas se encuentran menos cargados con peticiones de usuarios. En este sentido, es importante validar dos aspectos:

- **Que alguien supervisa que el proceso se ha ejecutado adecuadamente.** Por ejemplo, supongamos que un proceso actualiza cada noche la lista de precios y las posibles ofertas de mercancía. Alguien debe validar que realmente dichas listas se han actualizado correctamente cada mañana, o como mínimo, que, aunque el proceso se ejecute de noche, emita un aviso conforme ha terminado adecuadamente.

- **Que únicamente se planifican tareas aprobadas por los responsables adecuados.** De esta forma evitar, por ejemplo, que alguien pueda ejecutar cada hora el proceso de pago de nómina mensual. Por ello es importante restringir quién accede al planificador y asegurar que todo lo que hay dentro se encuentra aprobado.

La evaluación de este aspecto es complicada, dado que pueden existir procesos cuyo nombre no coincida o sea descriptivo de la función que cubren. Para una persona con conocimientos básicos no será fácil este punto.

Se debe verificar:

- **Que se encuentren aprobados.**

- **Que se hayan ejecutado de forma satisfactoria** (para una muestra de casos en función de su periodicidad, diario, semanal, mensual…).

- **Que las posibles incidencias se hayan resuelto adecuadamente.**

Ver MS7.PDF

Bibliografía:

Guía de Controles Generales de Sistemas de Información. ISACA "Barcelona Chapter".

Las Tecnologías de la Información y Comunicación en el aprendizaje. Consuelo Belloch.

UNE-ISO/TR 23081-3:2012 IN. Información y documentación. Metadatos para la gestión de documentos. Parte 3: Método de auto-evaluación.

Noma Internacional de Auditoría (NIA) en entornos Informatizados.