MÓDULO VIII

La Auditoría Informática en el entorno del Compliance

27 de Marzo de 2017

Curso Superior en Corporate Compliance.

Auditoría Informática

Proceso

Llevado a cabo por profesionales capacitados

Obtener evidencias

Objetivo: concluir sobre si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, y si lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas.

Herramientas ISACA

Parte 1: Grado de Complejidad de las Tecnologías de la Información en la Entidad.

(Ver documento adjunto *2- Papel de trabajo del grado de complejidad de TI.xlsx*)

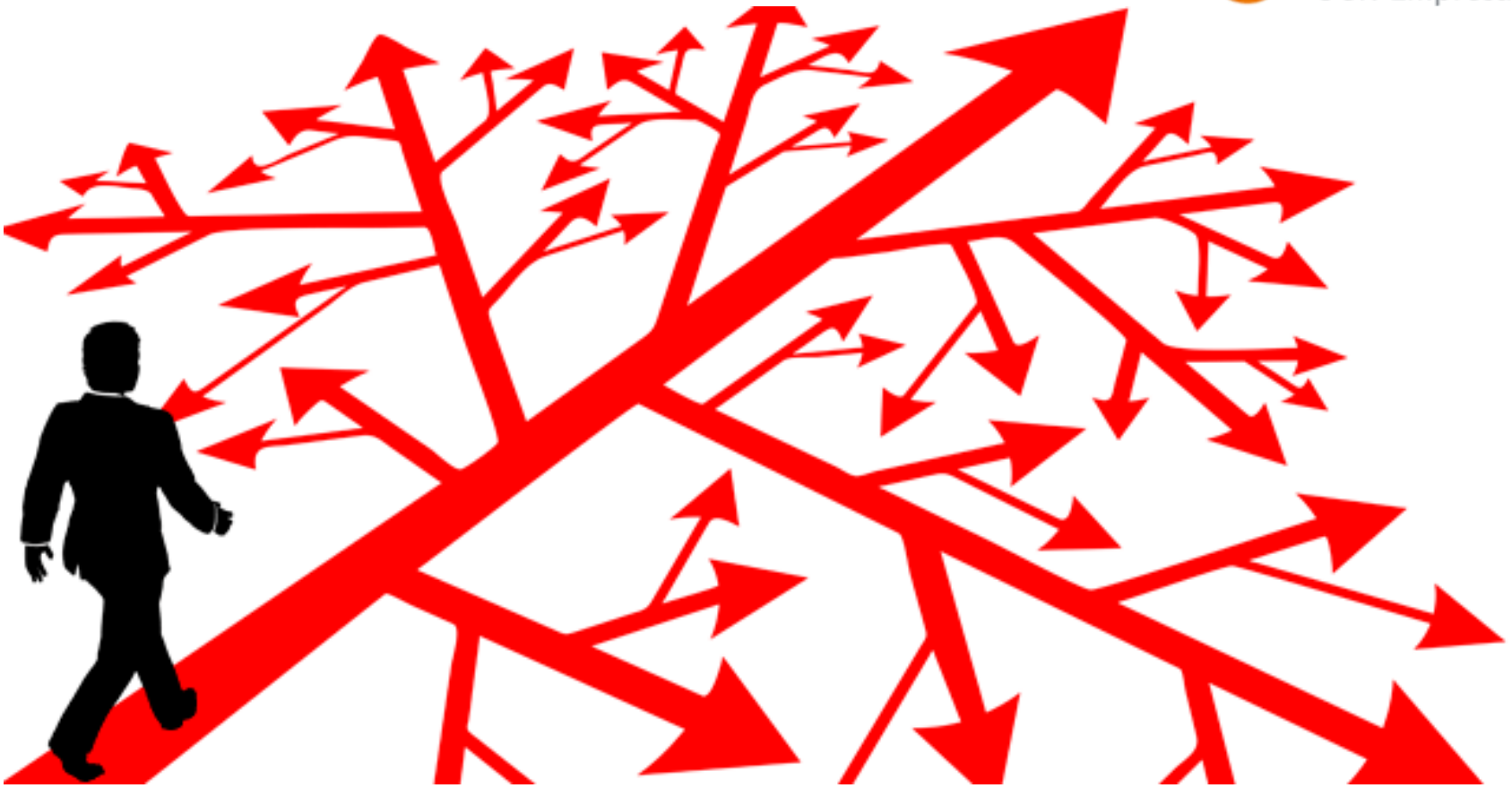
Parte 2: Controles Generales de TI.

(Ver documento adjunto *3- Papel de Trabajo de Controles Generales.xlsx*). Consta de 3 dominios:

2.1. Dominio 1. Seguridad Lógica y Física. (9 controles)

2.2. Domino 2. Proceso de desarrollo de aplicaciones, adquisiciones y nuevos desarrollos de aplicaciones. (11 controles).

2.3.- Dominio 3. Explotación de sistemas. (11 controles).



Determinación del grado de complejidad del entorno TI

Grado de complejidad. Estructura

2.1.1. Indicadores de Estructura

2.1.1.1. Servidores

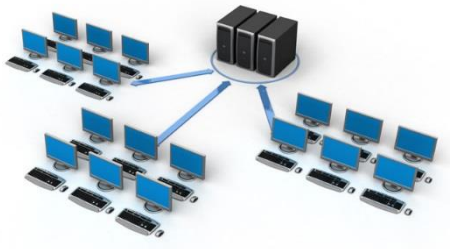
2.1.1.2. Sistemas Operativos

Windows Server

Mac OS

Linux

2.1.1.3. Estaciones de trabajo



Grado de complejidad. Organización

2.1.2. Indicadores de Organización

2.1.2.1. Departamento de TI

2.1.2.2. N.º de personas Dpto. TI

2.1.2.3. N.º de centros de datos.

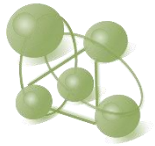
Grado de complejidad. Aplicaciones (Softwares)

2.1.4. Softwares o Aplicaciones

2.1.3.1. Aplicaciones de Negocio.

2.1.3.2. Adaptaciones a las aplicaciones.

2.1.2.3. "Interfaces" entre aplicaciones.



2.1.2.4. Frecuencia de modificaciones.

2.1.2.5. ¿Reportes estándares?

2.1.2.6. ¿Se necesitan varias aplicaciones para obtener los reportes?

Grado de complejidad. Complejidad

2.1.4. Indicadores de Complejidad

2.1.4.1. EDI

- El mensaje
- El software
- La comunicación

2.1.4.2. Comercio electrónico automatizado con clientes

Grado de complejidad. Externalización

2.1.5. Externalización Informática

2.1.5.1. En la gestión de aplicaciones.

2.1.5.2. En la gestión

- servidores,
- sistemas operativos,
- infraestructuras de red
- puestos de trabajo

Grado de complejidad.
Juicio profesional

Controles Generales del entorno TI

Controles Generales TI

Análisis del Riesgo

Test de Ayuda

Obtener evidencias

Objetivo: poder concluir, **en entornos informáticos de complejidad baja**, sobre la solvencia del mismo.

Material de referencia "Guía de Controles Generales de Sistemas de Información", y "PT Controles Generales.xls"

Controles Generales TI

Seguridad Lógica y Física

Proceso Desarrollo

Explotación de Sistemas

Seguridad

- **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.

Controles de Seguridad Lógica y Física

Seguridad Lógica y Física

- **Seguridad lógica:** Es la configuración adecuada del sistema para evitar el acceso no autorizados, ya sea a nivel local o vía red.

- **Seguridad física:** Es la seguridad que ofrece el entorno donde esta ubicado el equipo.

Seguridad Lógica y Física

SL1. Política de Seguridad:

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

Procedimientos de "bajo nivel"

- Mecanismos para **distinguir la información confidencial de la normal**.
- **Procedimientos de utilización de sistemas informáticos** (uso del correo, de internet…)
- **Cláusulas de confidencialidad** en caso de accesos externos a información.
- **Alta, modificación y eliminación de usuarios** en el sistema.
- **Mecanismos de control de acceso** lógico (quién puede acceder a qué).
- **Planificación de copias** de respaldo en caso de que se pierda algún fichero.
- **Mecanismos de seguridad física** (servidores innifugos, extintores…)
- **Procedimientos de aceptación de nuevos empleados** (revisión de credenciales antes de la contratación…)
- **Procedimientos de protección de los equipos informáticos** (antivirus, protección de red…)
- **Metodología de desarrollo de nuevas aplicaciones o modificaciones** sobre las existentes.

Seguridad Lógica y Física

SL2. Identificación de Usuarios:

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

Pruebas

- ¿Se dispone de alguna regla sobre nomenclatura de usuarios o normativa al respecto?
- Es importante que se puedan asociar los usuarios a personas concretas.
- Peligro ante los usuarios "genéricos" sin control.
- Pedir un listado de usuarios sobre procesos críticos (contabilidad, tesorería, RR.HH., …), hacer validaciones sobre la normativa interna.

Seguridad Lógica y Física

SL3. Política de contraseñas:

Comprobar si la organización ha definido controles de autenticación basados en la **existencia de contraseñas.**

Pruebas

- Que no se disponga de contraseñas "débiles".
- Caducidad.
- Bloqueo por intentos fallidos.
- Complejidad.
- Tiempo de inactividad.
- Longitud mínima y máxima de la contraseña.
- Histórico de contraseñas.

Seguridad Lógica y Física

SL4. Autorización de usuarios:

Comprobar si **los usuarios disponen de permisos en el sistema de acuerdo a las funciones que desempeñan**.

Pruebas

- **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.
- **Comprobar con el departamento de RR.HH.** (despido, cambio de puesto en la organización, nueva contratación…)

Seguridad Lógica y Física

SL5. Gestión de usuarios:

Comprobar si **existen 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**.

Pruebas

- **Todos los accesos deben ser autorizados por el responsable** de la información accedida.
- **El usuario tendrá acceso únicamente a la información que necesita para el desempeño de sus funciones**.
- Se deben cumplir requisitos de **segregación de funciones**.
- Se debe **pedir un listado con todos los usuarios y los accesos permitidos**, agrupados por perfiles y grupos lógicos. (contabilidad, administración, …)

Seguridad Lógica y Física

SL6. Usuarios administradores

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

Pruebas

- **¿Existen políticas específicas para los administradores de sistemas?**
- **Cumplimiento estricto de las medias dispuestas en SL2, SL3, SL4 y SL5**
- Comprobar que **no existen usuarios administradores con contraseñas "por defecto".**
- **Las personas con acceso ilimitados deberían ser las mínimas e imprescindibles.**

Seguridad Lógica y Física

SL7. Seguridad Física

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

Pruebas

- **Ambientales**: temperatura, detectores y extintores de incendios,
- **De acceso:** ¿en un lugar cerrado?
- **De ubicación**: evitar zonas bajas (por inundaciones…)
- **Fuentes de alimentación alternativas**. (SAI)
- **Limpieza.** No es una sala de trabajo.
- **Revisión de las medidas, de forma periódica**.

Seguridad Lógica y Física

SL8. Controles antivirus

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

Pruebas

- **Antivirus**: disponer de una herramienta actualizada.
- **De correo electrónico:**
- **De sistema:**

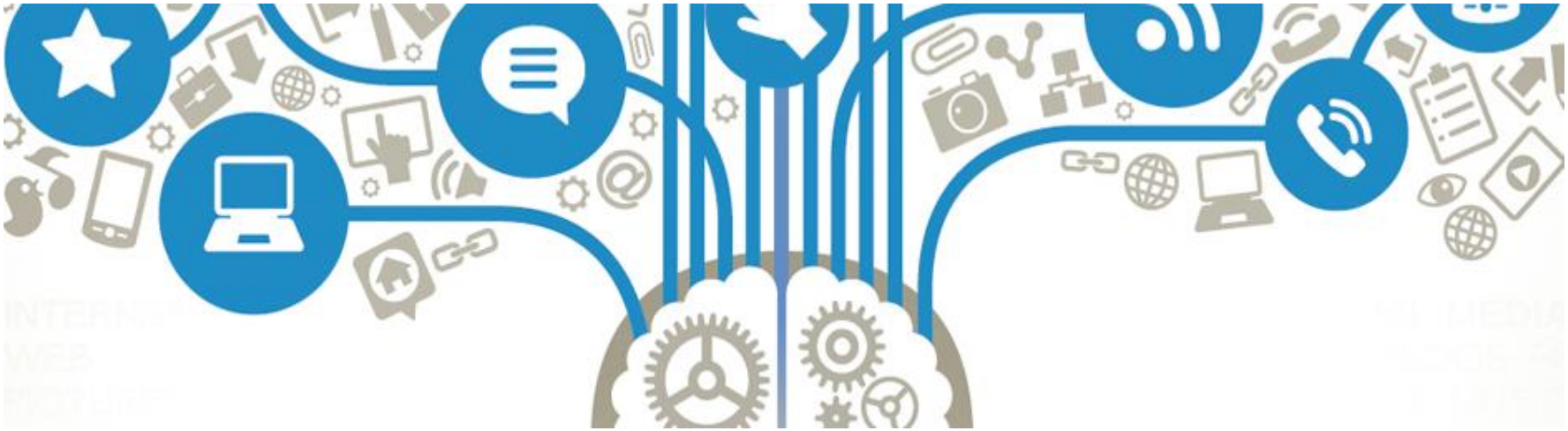
Seguridad Lógica y Física

SL9. Supervisión de la Seguridad

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

Pruebas

- **Revisión por una persona diferente**. (revisión sobre aspectos de SI1 a SL8)
- **Evidencia:** ¿existe un informe? Evaluar su contenido, su forma…
- **Comparación**: comparar nuestros hallazgos de auditoría con los aspectos puestos de manifiesto en ese informe de seguimiento.



Controles del área de Desarrollo

Controles de Desarrollo

PD1. 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.**

Pruebas

Debería existir una "**metodología de desarrollo**", y, al menos, contener:

- 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.

Controles de Desarrollo

PD2. Cambios autorizados

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

Pruebas

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.

Controles de Desarrollo

PD3. 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.**

Pruebas

Se debería contar con un proceso formal para la adquisición de aplicaciones o servidores:

- **Disponer de al menos tres opciones** de adquisición, correspondientes a distintos proveedores o soluciones. Las soluciones deben ser comparables entre sí.
- **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.

Controles de Desarrollo

PD4. Cambios de emergencia

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

Pruebas

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.**

Controles de Desarrollo

PD5. 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..**

Pruebas

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.**
- **Las herramientas disponibles para la evaluación (mapas de aplicaciones)**

Controles de Desarrollo

PD6. Entorno de pruebas

Comprobar si **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.**

Pruebas

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

- **Entorno de desarrollo.**
- **Entorno de integración.**
- **Entorno de pre-producción, o calidad.**
- **Entorno real, también denominado producción.**
- **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.**

Controles de Desarrollo

PD7. Selección de proveedores

Comprobar si **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.**

Pruebas

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

- **Selección de entre al menos, 3 opciones de proveedores.**
- **2 ó 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.**
- **Estudiar la "dependencia" de determinados proveedores.**

Controles de Desarrollo

PD8. Acuerdos de Nivel de Servicio

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

Pruebas

Consultar:

- **Si se dispone de contratos "estándar".**
- 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.**

Controles de Desarrollo

PD8. Acuerdos de Nivel de Servicio

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

Pruebas

Consultar:

- **Si se dispone de contratos "estándar".**
- 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.**

Controles del área de Explotación de Sistemas

Controles de Explotación

MS1. 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.**

Pruebas

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 cuánto?).
- **Tipo de las copias** (completas o incrementales).
- **Almacenamiento de las copias** (en cintas, en discos, pen drives…)
- **Retención de las copias** (cuánto tiempo se mantienen las copias)
- **Procedimiento de generación de copias de respaldo**.
- **Procedimiento de recuperación de información**, en caso necesario.

Controles de Explotación

MS2. Pruebas Periódicas de Copias de Seguridad

Comprobar si **la Organización prueba las copias de seguridad de forma periódica para asegurarse de que son utilizables en caso de emergencia.**

Pruebas

Esta suele contener la determinación sobre los siguientes puntos:

- **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.**

Controles de Explotación

MS3. 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.**

Pruebas

Se debe preguntar si existen:

- **Mecanismos para monitorizar el rendimiento de los equipos y de sus conexiones.**
- **Un procedimiento escrito.**
- **Actualizaciones sobre las versiones de softwares.**

Controles de Explotación

MS4. 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.**

Pruebas

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

- **Mecanismos de detección.**
- **Registro.**
- **Asignación.**
- **Priorización/Criticidad.**
- **Gestión y resolución.**
- **Aprobación.**
- **Escalado.**
- **Seguimiento.**

Controles de Explotación

MS5. 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.**

Pruebas

Se debe preguntar qué herramientas soporte son críticas. Se deberá consultar sobre los siguientes aspectos:

- **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.**
- **Si existe un control de versiones.**

Controles de Explotación

MS6. Traspasos de información

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

Pruebas

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.**

Controles de Explotación

MS7. Ejecución de 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.**

Pruebas

Para una muestra de procesos, se debería 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.**