Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Procedimiento de Auditorías Internas

Procedimiento de Auditorías Internas		
CONTROL DE VERSIONES		
Versión inicial		**Fecha**
V.1.0		**19/03/2019**
Documento elaborado por		
Responsable de actualización		
Versiones Posteriores	**Cambio realizado**	**Fecha**
Estado	**Aprobado por :**	
Etiquetado del documento	**Uso Interno**	

LISTA DE DISTRIBUCIÓN

Este documento ha sido distribuido a los siguientes responsables:

Nombre	Responsabilidad

COPYRIGHT

Tabla de contenido

1. Objeto y campo de aplicación

El objeto del presente procedimiento es realizar un examen sistemático e independiente al Sistema de Gestión implantado para determinar su correcta aplicación y eficacia, identificando anomalías y posibles mejoras o correcciones.

Estas auditorías internas deberán realizarse por lo menos una vez al año en todas las áreas implicadas en el SGSI con el fin de determinar si los objetivos, los procesos, procedimientos y los controles y activos están conformes con:

- Los requisitos de las normas internacionales bajo las que se ha desarrollado el sistema y la correspondiente legislación en vigor.
- Los requerimientos particulares del Sistema de Gestión.
- Además se comprobará:
    - Si el Sistema de Gestión alcanza los niveles esperados.
    - Los resultados de auditorías previas.
    - Si el Sistema está correctamente implantado y mantenido de manera eficaz.

2. Responsabilidades

El Responsable del SGSI tiene la obligación de realizar:

- El programa de auditoría.
- La selección del equipo auditor, integrado por personal propio o externo, en representación de la organización, pero en ningún caso por personal del departamento, sección o área que vaya a ser auditada, para asegurar la objetividad e imparcialidad del proceso.
- Asegurarse de la formación y cualificación de los auditores internos, conforme a los requisitos y programas de instrucción que a tal fin se desarrollen.
- La distribución del informe de auditoría a los responsables de los departamentos auditados y a la Dirección Ejecutiva.
- El establecimiento de las acciones correctivas a las incidencias o no conformidades detectadas durante la auditoría.
- El seguimiento de la puesta en práctica de las acciones correctivas previstas y la verificación, junto con su resultado, de las soluciones acordadas en el plazo de tiempo establecido.

El equipo Auditor es responsable de:

- La realización de los planes de auditoría.
- La realización de la auditoría.
- La emisión de los informes de auditoría.

3. Desarrollo

3.1. Planificación de la auditoría

El Responsable del SGSI tiene la máxima autoridad y responsabilidad en todos los asuntos relativos a la implantación, ejecución y administración del SG, pudiendo ordenar la realización de auditorías sobre cualquier punto de dicho sistema, en cualquier momento.

Periódicamente, el Responsable del SGSI programa y planifica las auditorias a realizar, de acuerdo con los requisitos de auditoría del SGSI. Esta programación se documenta basándose en:

- Certificación del SGSI.

- Cambios en el contexto de la organización.
- Cambios producidos en el alcance SGSI.
- Cambios derivados de nuevas tecnologías.
- Resultados de auditorías anteriores.
- Evolución de los indicadores/métricas.
- No Conformidades.
- Incumplimiento legal, regulatorio o contractual.
- Se produzcan situaciones que así lo requieran por ejemplo: incidentes graves de seguridad, eventos de entorno con posibles consecuencias graves, daños a la imagen, etc.
- Criticidad del área afectada.
- Resultado de auditorías anteriores.
- Innovaciones producidas en relación con personas.
- Cambios en la evaluación de riesgos y políticas, etc.

3.2. Formación de auditores

Para la realización de las auditorías internas a cualquiera de las áreas de la organización se dispone de un personal auditor debidamente formado y entrenado, y ajeno al área que se ha de auditar, para garantizar así la independencia y la objetividad de la auditoria. En los casos que el Comité de Dirección lo estime necesario, se contrata para esta actividad a personal externo a la organización que cumpla los requisitos especificados.
Los requisitos que se requieren para realizar una auditoría en la organización quedan descritos en el perfil de puesto rol del mismo.

3.3. Realización de la auditoría

Las auditorías se planificación a intervalos, y se efectúa siguiendo el "Plan de auditoría" (**TFM_REG_PLAN DE AUDITORIA**). Dicho plan de auditoría debe contener como mínimo los siguientes puntos:

- Fecha de auditoría,
- Equipo auditor,
- Alcance del Sistema de gestión,

- Procesos negocio y/o actividad a auditar,
- Responsables involucrados,
- Normas de referencia y otros requisitos,
- Desglose detallado y cronológico de las actividades a realizar,
- Selección de controles, etc.

Este plan deberá ser enviado por parte del auditor antes de la fecha prevista de ejecución de la auditoría interna, al Responsable del SGSI, a fin de que informe del programa a los involucrados, con el propósito de comprobar su disponibilidad y poder establecer el programa definitivo.
El equipo auditor deberá cumplir en lo posible con el plan de auditoría y el programa establecido, o en su defecto, indicar en el informe las desviaciones respecto al plan.

Se podrá utilizar en caso necesario una lista de comprobación, pero sin restringir la investigación a otros posibles aspectos de interés o dudosos, que surjan durante la realización de la misma y teniendo en cuenta que durante el desarrollo de la auditoria los responsables de cada proceso deberán proporcionar a los auditores evidencias del desarrollo de los mismos como por ejemplo:

- Políticas que afecten al alcance del sistema.
- Planes de gestión de riesgos.
- Registros de incidencias en materia de seguridad.
- Cumplimiento y seguimiento de objetivos y controles.
- Informe de la auditoria anterior.
- Registros de No Conformidades, Acciones Correctivas, Acciones Preventivas.
- Registros y certificados establecidos por la Ley.
- Cualquier informe o comunicación de obligado cumplimiento en materia de seguridad de la información.
- Informes de revisión del sistema por el Comité de Dirección de Seguridad.
- Listado de Requisitos Legales y Contractuales.
- Cumplimiento de la documentación: Instrucciones de trabajo, procedimientos, manuales y otros documentos de aplicación al alcance evaluado, mediante la presentación de los registros cumplimentados.
    - Otros:
        - Se revisan las operaciones y documentos relacionados con el Sistema de Gestión, que se manejen en el punto auditado.

- Se comprueba la realización de las distintas operaciones propias del punto auditado, comparándose la misma con lo establecido en los procedimientos u otros documentos aplicables, en los que se especifica la actividad a realizar y el modo de hacerlo.
- Se examinan y evalúan solamente evidencias objetivas que se pueden verificar, evitando las impresiones subjetivas y las conclusiones no contrastadas.
- En caso de encontrar una posible no conformidad, se investiga más profundamente para confirmarla y averiguar si es o no sistemática e identificar causas y efectos.
- Se anotan todos los detalles posibles sobre los aspectos comprobados y las deficiencias o no conformidades detectadas con anterioridad a la auditoría.
- Se practica un seguimiento exhaustivo de los asuntos pendientes y no conformidades en anteriores auditorías.
- Se comprueban los niveles de protección implantados, su conformidad con las especificaciones, y si éstas son importantes, comprobar que hayan sido probadas.

A continuación, el equipo auditor y el auditado mantienen una reunión con el objeto de:

- Aclarar las posibles dudas o confusiones.
- Comentar los resultados.
- Emitir, si procede, los informes de no conformidad.

De las no conformidades detectadas en el "Informe de Auditoría", los responsables de los departamentos afectados, junto con el Responsable del SGSI, las registrarán y planificarán las acciones derivadas (inmediatas y correctivas).
De las observaciones o propuestas de mejora detectadas en el "Informe de Auditoría", la empresa estudiará la conveniencia o no de tomar las acciones oportunas, con el fin de mejorar el Sistema de Gestión.

El Responsable del SGSI tratará de asegurarse de que toda la documentación y software al que tenga acceso el auditor (en caso de ser necesario), tanto para la preparación como durante la realización de la auditoría, está en modo "sólo lectura". Si no fuera posible o no se estimara adecuado el Responsable del SGSI podrá realizar una copia aislada de dicha información que será eliminada cuando finalice la auditoría.

3.4. Informe de la Auditoría

Por cada auditoría llevada a cabo, el auditor rellena el "Informe de auditoría interna", que pone en evidencia las diferencias entre los elementos esperados y los realmente encontrados durante las auditorías.
Los informes de auditoría son entregados por el Equipo Auditor al Responsable del SGSI, y éste informará a los responsables de los departamento/áreas auditados para que propongan, si procediera, acciones correctivas.
Asimismo, las conclusiones serán informadas al Comité de Dirección de Seguridad siguiendo las revisiones planificadas establecidas.
Las no conformidades de la auditoría se tratarán de acuerdo al procedimiento (TFM_PROC_Gestión de No Conformidades Acciones Correctivas y de Mejora

4. Registros y Archivo

Se consideran registros del SGSI los siguientes:

Nombre del Registro	Responsable	Tipo de archivo	Periodo mínimo
TFM_REG_Programa de Auditoria	Responsable del SGSI	Electrónico	3 años
TFM_REG_Plan de Auditoría	Responsable del SGSI	Electrónico	3 años
Informe de Auditoría	Responsable del SGSI	Electrónico	3 años

5. Referencias

- TFM_PROC_Gestión No Conformidades Acciones Correctivas y de Mejora