Evaluación, Auditoría y Certificación

Las certificaciones tienen los siguientes beneficios:

- Mejor seguridad a menor coste
- Credibilidad y confianza: Muestra que se han tomado las precauciones requeridas para minimizar los riesgos del negocio
- Cumplimiento: Demuestra cumplimiento con regulaciones
- Cumplir responsabilidades de confianza como organización en la protección de los activos de la compañía.

Cumplimiento, Certificación y Acreditación

- Cumplimiento: Cualquier organización puede implementar un estandar y decir que cumple, pero no hay ninguna evidencia
- Certificación: Es una forma de probar que la organización cumple con los estándares.
- Acreditación: Se le entrega a la organización que realiza la certificación. Los cuerpos de certificación tiene que demostrar que sus métodos de certificación son justos, creibles y confiables, para ello suelen haber autoridades de acreditación nacionales.

Certificación y Acreditación en España

En españa está la Entidad Nacional de Acreditación (ENAC). Tiene los siguietes servicios de acreditación:

- Certificación de los Sistemas de Gestión de la seguridad (ISO27001): Asegura la confidencialidad, integridad y disponibilidad de la información..
- Certificación dentro del Esquema Nacional de Seguridad (ENS): Fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la adminsitración pública.

ISO 27001

ISO 27001: La Certificación

Se suelen seguir los siguientes pasos:

- Pre-auditoría: Existencia y alcance apropiado del SGSI
- Auditoría de certificación
    - Fase 1: Revisión de la documentación
    - Fase 2: Procesos y control
- Certificación: Emisión del certificado
- Seguimiento anual: Mejora continua.

ISO 27001: El ciclo de certificación

1. Revisión de preparación
2. Certificación
3. Auditoría de supervisión: Comienza el cliclo, estas auditorías revisan las auditorías internas, gestión de las revisiones, acciones correctivas y preventivas, mejoras...
4. Auditoría de recertificación: Revisa el sistema completo de forma menos profunda que la primera audotoría, centrándose en las capacidades de mejora.

Documentos y registros necesarios

1. Alcance del sistema de gestión de seguridad de la información
2. Política de seguridad de la información
3. Proceso de evaluación de riesgos
4. Proceso de tratamiento de riesgos
5. Objetivos de seguridad de la información
6. Evidencia de la competencia de las personas que trabajan en SI
7. Otros documentos relacionados con el SGSI considerados necesarios en la organización
8. Documentos de planificación y control operacional
9. Resultados de las evaluaciones de riesgo
10. Decisiones con respecto al tratamiento del riesgo
11. Evidencia del seguimiento y medición de seguridad de la información
12. Porgrama de auditoría interna sobre SGSI y sus resultados
13. Evidencia de las principales revisiones de la gestión del SGSI
14. Evidencia de las no conformidades identificadas y acciones correctivas que surjan

Problemas comunes

- Registro de activos incompleto
- Riesgo del personal no incluido
- Métodos demasiado complicados
- No aprobado por gerencia
- Ubicación de la sala de servidores
- Sala de servidores no segura
- Incidentes no reportados por el personal
- Pruebas insuficientes para demostra mejora

Esquema Nacional de Seguridad (ENS)

RD 3/2010 Artículo 34: Auditoría de seguridad

- Los sistemas de información serán objeto de una auditoría regular ordinaria al menos cada 2 años para verificar el cumplimiento de los requerimientos del ENS
- Se debe realizar una auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de la información.

La adecuación al ENS requiere el tratamiento de las siguientes cuestiones:

- Definición de roles y la asignación de responsabilidades (CCN-STIC 805)
- Categorizar los sistemas (CCN-STIC 803)
- Realizar análisis de riesgo y valoración de las medidas de seguridad existentes (MAGERIT Versión 3 y PILAR)
- Declaración de aplicabilidad (CCN-STIC 804)
- Plan de adecuación para la mejora de la seguridad (CCN-STIC 806)
- Implantar, operar y monitorizar las medidas de seguridad (CCN-STIC)
- Auditar la seguridad (CCN-STIC 802 y CCN-STIC 808)
- Informar sobre el estado de la seguridad (CCN-STIC 815 y CCN-STIC 824)

Consejo de Certificación del ENS (CoCENS)

Organo colegiado, regulado por la sección 3 del capítulo II del título preliminar de la Ley 40/2015 y por la guia CCN-STIC 809 de Declaración y Certificación de Conformidad con el ENS. Fue creado para ayudar a la implantación del ENS. Hay los siguientes informes CoCENS:

- CCN-CERT IC-01/19: Criterios generales de auditoría y certificación
- CCN-CERT IC-02/20: Guia para la contratación de auditorías de certificación del ENS

La Certificación y conformidad con el ENS conlleva:

- **1. Plan de adecuación: Documento que incluye la siguiente info**:
  - **Alcance** de los sistemas que se van a someter al proceso de certificación
  - **Categoría** de los sistemas según las dimensiones de seguridad y los servicios rpestados
  - **Declaración de Aplicabilidad Provisional**, teniendo en cuenta las medidas del anexo II que se va a implementar.
  - Realización del **análisis de riesgos**
  - Validar la **declaración de aplicabilidad definitiva**
  - Preparar y aprobar la **política de seguridad**.
- **2. Implementación de la seguridad**
  - **Hoja de ruta**: Documento a elaborar, medidas técnicas a implementar y definir las prioridades
  - Elaborar el **marco normativo** y la implantación de la seguridad
  - Aprobar el **sistema de gestión de la seguridad de la información**
- **3. Declaración/Certificación de conformidad**
  - **Catetgorías MEDIA o ALTA**: Auditoría formal que verifique los requerimientos del ENS cada 2 años o antes si se producen cambios
  - **Categoría BÁSICA:** Autoevaluación que verifique su cumplimiento al menos cada 2 años.
- **4.Informar sobre el estado de la seguridad**
  - **Métricas e indicadores**: Se debe cumplomentar e informar sobre el estado de la seguridad.
- **5. Vigilancia y Mejora Continua**
  - Revisión de la política de seguridad de la información
  - Revisión de la información y los servicios
  - Actualización del análisis de riesgos
  - Revisión de la declaración de aplicabilidad
  - Realizar Auditorías internas
  - Revisión del plan de mejora
  - Revisión de las medidas de seguridad

    - Revisión y actualización de procedimientos
    - Revisión del estado de seguridad

Auditoría

Es un proceso sistemático, independiente y documentado para obtener evidencias y evaluar el objetivo para determinar hasta que extensión se han cumplido los objetivos a auditar. En las auditorías existen los siguientes fundamentos:

- Evidencia auditada: Registro verificable, afirmación o hecho relevante para la auditoría
- Descubrimientos de la auditoría: Resultados de la evaluación de las evidencias recolectadas
- Conclusiones de la auditoría: Resultado de la auditoría tras considerar los objetivos de la auditoría y los descubrimientos
- Cliente auditado: Organización que solicita la auditoría.
- Auditado: Organización que es auditada
- Auditor: Los que realizan la auditoría.

Auditoría Interna

También conocidas como First-Party. Son realizadas en nombre de o por la organización para revisar la gestión y otros propósitos.

Auditoría externa

También conocidas como second-party o thir-party. Las Second party son realizadas por grupos interesados en la organización. Las Third Party son realizadas por organizaciones auditoras independientes.

- ISO/IEC 27007:2011 Guidelines for information security management system auditing
- ISO/IEC TR 27008:2011: Guidelines for auditors on iformation security controls

Auditorías combninadas

- Auditoría combinada: Cuando 2 o más sistemas de gestión de diferentes disciplinas son auditados juntos
- Auditoría Conjunta: Cuando 2 o más organizaciones cooperan para auditar una organización.

Principios para auditores y gestores de auditorías

- Integridad: Deben ser honestos. Deben observar y respetar cualquier requerimiento legal aplicable. Deben demostrar competencia técnica.
- Presentación justa: Deben reportar de forma correcta y precisa.
- Importancia por el profesionalismo: Aplicación diligente de la auditoría.
- Confidencialidad

Principios del proceso de auditoría

- Independencia: La base para la imparcialidad de la auditoría
  - Los auditores deben ser independeintes de la actividad auditada de forma que no hayan conflictos de interés
  - Para las auditorías internas, los auditores deben ser independientes de los gestores de las funciones auditadas
  - Para las organizaciones pequeñas puede no ser posible que los auditores internos sean completamente independientes de la actividad auditada
- Proximación basada en evidencias.
  - Las evidencias de las auditorías deben ser verificables
  - Las evidencias tienen que ser basadas en muestras de la información disponible.

Estudio de alcance y pre-auditoria

- Los auditores determinan las principales areas en las que centrar las auditorías y las áreas que quedan expecíficamente fuera
- El alcance de la auditoría tiene que tener sentido en relación con la organización
- Prestar atención a los riesgos de la información y los controles de seguridad asociados con la información
- Identificar y hacer contacto con los principales interesados

Planificación y preparación de la auditoría

- El alcance ISMS negociado se divide en mayor detalle, generando una checklist ISMS
- El tiempo y recursos para la auditoría son negociados por la gerencia de ambas organizaciones
- Los planes de audotría suelen incluir checkpoints.