CONCEPTOS DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN. NORMA ISO 27000.

Estándares de gestión de la seguridad de la información

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Muchos de ellos no están aún publicados, pero la estructura ya está definida:

- ISO/IEC 27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009.
- UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI).
- Requisitos. (ISO/IEC 27001:2005), publicada en el año 2007. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información.

Estándares de gestión de la seguridad de la información

- ISO/IEC 27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, última versión publicada en el año 2013.

  Esta guía de buenas prácticas está organizada en 14 dominios, 35 objetivos de control y 114 controles recomendables en cuanto a seguridad de la información.
- ISO/IEC 27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
- ISO 27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

Estándares de gestión de la seguridad de la información

- ISO/IEC 27005:2008 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008.

  Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.
- ISO/IEC 27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Publicada en el año 2007.

  Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.

Estándares de gestión de la seguridad de la información

- ISO/IEC 27007. Guía para la realización de las auditorías de un SGSI.
- ISO/IEC 27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002.

  Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO 27001 y conseguir un nivel de seguridad aceptable.
- EN ISO 27799. Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC 27002 (ISO 27799:2008).

  Vigente en nuestro país ya que ha sido ratificada por AENOR en agosto de 2008. Como en la anterior, es una guía sectorial que da cabida a los requisitos específicos de entorno sanitario.

Estándares de gestión de la seguridad de la información

- La norma UNE-ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización
- La Norma recoge:
  - **Los componentes del SGSI**, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuales son los registros que permitirán evidenciar el buen funcionamiento del sistema.
  - **Cómo se debe diseñar e implantar el SGSI**.
  - **Define los controles de seguridad a considerar**. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
  - **Cómo debe realizarse la revisión y mejora del SGSI**.

Implantación de un SGSI

1. Fase PLAN

Planificar y diseñar el SGSI según la Norma UNE/ISO-IEC 27001 implica:

- **Establecer alcance del SGSI. Es el primer paso. Hay que decidir qué parte de la organización va a ser protegida.**
- **Establecer las responsabilidades. Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad.**
- **Definir política de seguridad. Este paso es fundamental. La política de la organización es la que va a sentar las bases de lo que se va a hacer, mostrará el compromiso de la dirección con el SGSI y servirá para coordinar responsabilidades y tareas.**

Implantación de un SGSI

1. Fase PLAN

Planificar y diseñar el SGSI según la Norma UNE/ISO-IEC 27001 implica:

- **Realizar análisis de riesgos**. El análisis de riesgos es la piedra angular de un SGSI. Es la actividad cuyo resultado nos va a dar información de dónde residen los problemas actuales o potenciales que tenemos que solucionar para alcanzar el nivel de seguridad deseado. El análisis de riesgos debe ser proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que los activos están expuestos.
- **Seleccionar los controles**. Una vez que se sabe dónde están los puntos débiles en la gestión de la seguridad, se escogen los controles necesarios para eliminarlos o al menos, reducir la probabilidad de que ocurran algún incidente o el impacto que tendría en caso de que algo ocurriera. En principio los controles se escogerán de los detallados en el Anexo A de la Norma.

Implantación de un SGSI

1. Fase PLAN

Planificar y diseñar el SGSI según la Norma UNE/ISO-IEC 27001 implica:

- **Establecer el plan de seguridad**. Debido a que serán numerosas las actuaciones que se pretenderá realizar, debe establecerse un plan con los plazos, los recursos y las prioridades a la hora de ejecutarlas.

Implantación de un SGSI

2. Fase DO (Hacer)

En esta fase debe llevarse a efecto el plan de seguridad planteado en la fase anterior.

- **Los principales documentos a generar son:**
  - **Política de seguridad. Con las líneas generales que la organización desea seguir en seguridad.**
  - **Inventario de activos. Con la descripción de los activos de información de la organización y su valoración para la misma.**
  - **Análisis de riesgos. Con los valores de riesgo de cada uno de los activos.**
  - **Documento de aplicabilidad. En el que se recoge para cada control del Anexo A de la Norma UNE/ISO-IEC 27001 si se aplica o no y la justificación para esa decisión.**

Implantación de un SGSI

2. Fase DO (Hacer)

En esta fase debe llevarse a efecto el plan de seguridad planteado en la fase anterior.

- Los principales documentos a generar son:
  - **Procedimientos**. Con la descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI.
  - **Registros**. Son las evidencias de que se han realizado las tareas definidas para el GSI. Son muy importantes de cara a poder medir la eficacia de las medidas implantadas así como a justificar las labores realizas frente a las auditorías del sistema (tanto internas como externas).

Implantación de un SGSI

3. Fase Check (Comprobar)

Una vez puesto en marcha el plan de seguridad, se debe revisar periódicamente de manera que se detecten posibles desviaciones.

Tiene por objeto la medida y evaluación de la eficacia de otros controles, mediante la auditoría se determinar si los objetivos de los controles, los controles, los procesos y los procedimientos:

- Están conformes con los requisitos de la Norma UEN/ISO-IEC 27001.
- Están conformes con la legislación y regulaciones aplicables.
- Están conformes con los requisitos de seguridad identificados.
- Están implementados y mantenidos de manera efectiva.
- Dan el resultado esperado.

Implantación de un SGSI

4. Fase Act (Actuar)

Hay tres maneras de actuación:

- **Adoptar acciones correctoras**. Estas acciones son las que se toman para corregir una no-conformidad significativa con los requisitos del SGSI.
- **Adoptar acciones preventivas**. Son aquellas que se toman para prevenir que ocurra algo no deseado. La gran ventaja de estas acciones es que evidentemente es más eficaz y sencillo prevenir los problemas que solucionarlos.
- **Definir acciones de mejora**. Las acciones de mejora no surgen de la necesidad de solucionar un problema sino de la dinámica del sistema de gestión, que impulsa a refinar procesos y superar objetivos continuamente. Son acciones encaminadas a hacer mejor las cosas de una manera más eficaz y eficiente, consiguiendo los resultados esperados con menos esfuerzo.

Análisis y valoración de los riesgos. Metodologías

Conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información:

- Amenaza: es la causa potencial de un daño a un activo.
- Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.
- Impacto: consecuencias de que la amenaza ocurra.
- Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.
- Salvaguarda: Medida técnica u organizativa que ayuda a paliar el riesgo.
- Riesgo residual: Riesgo remanente tras la aplicación de salvaguardas.

Análisis y valoración de los riesgos. Metodologías

- ***El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos***.
- A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles.
- Hay que tener en cuenta que la realización de un análisis de riesgos es un proceso laborioso. *Para cada activo se van a valorar todas las amenazas que pueden afectarle, la vulnerabilidad cada una de las amenaza y el impacto que causaría la amenaza en caso de ocurrir*. Con todos esos datos, se calcula el valor del riesgo para ese activo.

Proceso de certificación

- **Certificar un SGSI según la Norma UNE/ISO-IEC 27001 significa obtener un "Documento" que reconoce y avala la correcta adecuación del Sistema de Gestión de Seguridad de la Información conforme a esta norma de referencia.**
- **La realización de las auditorías de un SGSI se rige por la Norma ISO/IEC 27006, que determina los requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información.**

Proceso de certificación

- **La auditoría suele constar de dos fases:**
  - **Fase 1. Durante esta fase, los auditores deben revisar la documentación del SGSI para comprobar si la organización cuenta con un sistema lo suficientemente maduro y completo como para superar la Fase 2.**
  - **Fase 2. En esta fase los auditores deben confirmar que la organización cumple con sus políticas, objetivos y procedimientos y que el SGSI es eficaz. Para todo ello se realizaran pruebas de cumplimiento, es decir, se buscarán evidencias del cumplimiento de las normas establecidas por la organización.**
- **Una vez superada la auditoría de certificación y en su caso, la auditoría extraordinaria, se obtiene el certificado, que es válido para 3 años, aunque esta sujeto a la realización de una auditoria de seguimiento cada año.**

Informe de auditoría de seguridad. ISO 27002:2013

- El informe de la auditoría de seguridad está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013.
  - http://iso27000.es/iso27002.html
- Los controles que se definen son los siguientes:

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para la seguridad de la información.

Informe de auditoría de seguridad. ISO 27002:2013

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.

6.1.1 Asignación de responsabilidades para la segur. de la información.

6.1.2 Segregación de tareas.

6.1.3 Contacto con las autoridades.

6.1.4 Contacto con grupos de interés especial.

6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.

6.2.1 Política de uso de dispositivos para movilidad.

6.2.2 Teletrabajo.

Informe de auditoría de seguridad. ISO 27002:2013

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.

7.1.1 Investigación de antecedentes.

7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.

7.2.1 Responsabilidades de gestión.

7.2.2 Concienciación, educación y capacitación en segur. de la información

7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.

7.3.1 Cese o cambio de puesto de trabajo.

Informe de auditoría de seguridad. ISO 27002:2013

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.

- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.

- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.

- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

Informe de auditoría de seguridad. ISO 27002:2013

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.

- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.

- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

- 9.3.1 Uso de información confidencial para la autenticación.

Informe de auditoría de seguridad. ISO 27002:2013

9. CONTROL DE ACCESOS.

9.4 Control de acceso a sistemas y aplicaciones.

- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

Informe de auditoría de seguridad. ISO 27002:2013

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.

- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.

- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

Informe de auditoría de seguridad. ISO 27002:2013

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.

12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.

12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.

12.4.1 Registro y gestión de eventos de actividad.

12.4.2 Protección de los registros de información.

12.4.3 Registros de actividad del administrador y operador del sistema.

12.4.4 Sincronización de relojes.

Informe de auditoría de seguridad. ISO 27002:2013

12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

Informe de auditoría de seguridad. ISO 27002:2013

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

Informe de auditoría de seguridad. ISO 27002:2013

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

14.1 Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

14.2.1 Política de desarrollo seguro de software.

14.2.2 Procedimientos de control de cambios en los sistemas.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4 Restricciones a los cambios en los paquetes de software.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.

14.2.7 Externalización del desarrollo de software.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.

14.3.1 Protección de los datos utilizados en pruebas.

Informe de auditoría de seguridad. ISO 27002:2013

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.

15.1.1 Política de seguridad de la información para suministradores.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

Informe de auditoría de seguridad. ISO 27002:2013

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

16.1.1 Responsabilidades y procedimientos.

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.

Informe de auditoría de seguridad. ISO 27002:2013

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

Informe de auditoría de seguridad. ISO 27002:2013

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.

18.2.1 Revisión independiente de la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

18.2.3 Comprobación del cumplimiento.

Informe de auditoría de seguridad. ISO 27002:2013

- La legislación que deben aplicar es la siguiente:
  - Ley Orgánica de Protección de Datos (LOPD) + normativas de protección de datos
    - REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (GDPR en Inglés)

      http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php
  - Ley de Servicios para la Sociedad de la Información y el Comercio Electrónico (LSSI-CE)
  - Legislación de Firma Electrónica (LFE)

Relacionadas:

- Ley de Acceso de los Ciudadanos a los Servicios Públicos
- Ley de Medidas de Impulso a la Sociedad de la Información