CAPITULO II

La norma ISO 27001

Aspectos clave de su diseño e implantación

SIS-254 SEGURIDAD DE LA INFORMACION

Prof: Ing. D. Roca

FAMILIA ISO 27000

ISO International Organization for Standardization

ISO 27001

Es la norma principal de toda la serie ya que incluye todos los requisitos de un **Sistema de Gestión de Seguridad de la Información** en las organizaciones. Es la certificación que deben obtener las organizaciones. *Norma que especifica los requisitos para la implantación del SGSI*. **Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos**.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

Fue publicada como estándar internacional en octubre de 2005. Revisada en septiembre de 2013. En el Anexo A se enumeran los objetivos de control y los análisis que desarrolla la **norma ISO27001** para que se puedan seleccionar las empresas durante el progreso de sus **Sistemas de Gestión de Seguridad de la Información.**

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

LAS AMENAZAS A LOS ACTIVOS DE INFORMACIÓN

En la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de diversos focos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

LAS AMENAZAS A LOS ACTIVOS DE INFORMACIÓN

La seguridad de estos activos de información está en función de la correcta gestión de una serie de factores como: la capacidad, la elaboración de un plan de contingencia frente a los incidentes, el análisis de riesgos, las competencias, el grado de involucración de la Dirección, las inversiones en seguridad y el grado de implementación de controles.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

Aspectos claves de un SGSI basado en la norma ISO 27001

La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.

Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

ISO 27001

Como ocurre con todas las normas ISO, la 27001 es un sistema basado en enfoque del ciclo de mejora continua. Dicho ciclo consiste, como ya sabemos, en **Planificar-Hacer-Verificar-Actuar,** por lo que se le conoce también como ciclo **PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).**

FAMILIA ISO 27000

ISO International Organization for Standardization

PLANIFICAR	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias (involucra) Establecer un mapa de procesos Definir autoridades y responsabilidades
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles
CONTROLAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en ver indicadores y métricas, medir Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

ISO 27001

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

Relación de la norma ISO 27001 con la ISO 22301 y la ISO /IEC 20000

La norma ISO 27001, que como hemos visto está muy enfocada en la parte informática de la empresa, se encuentra muy ligada y tiene puntos en común con otras dos normas ISO: la ISO 22301 de continuidad del negocio y la ISO/IEC **20000,** de gestión de servicios TI (Tecnología de la Información).

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

La ISO 22301 trabaja el tema de la seguridad en la empresa desde una perspectiva mucho más general y global, tratando de asegurar la continuidad del negocio, lo cual influye en aspectos tan diversos como: los activos financieros, la contabilidad, los aspectos legales y todos los factores ligados con la producción y la operativa.

El estándar 22301 se centra en diversos aspectos de la organización que van a permitir su sustentabilidad, utilizando para ello ciertos elementos y controles que van a evitar las consecuencias de las distintas amenazas, así como también encontrar las causas que motivan el problema.

Un aspecto muy importante de la norma ISO 22301, que no tiene en cuenta la 27001, son los tiempos de recuperación, una cuestión crucial para poder evaluar si nuestro plan de contingencia es el adecuado para poder reanudar la actividad

en unos niveles aceptables para la organización, una vez ha ocurrido el incidente.

Otra norma relacionada con la ISO 27001 es el estándar ISO/IEC 20000, de gestión de la calidad de los servicios TI (Tecnologías de la Información): hosting, páginas web, elearning, desarrollo de software. Todo ello va ligado a la continuidad del negocio y de los servicios de información y, en conjunto, sirve para garantizar un servicio seguro, sin interrupciones importantes y de calidad.

FAMILIA ISO 27000

FASES DE UN SGSI BASADO EN LA NORMA ISO 27001

En base a este sistema PDCA, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI

1. Análisis y evaluación de riesgos.
2. Implementación de controles
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora
4. Alcance de la gestión
5. Contexto de organización
6. Partes interesadas
7. Fijación y medición de objetivos
8. Auditorías internas y externas
9. Proceso documental(conclusiones y recomendaciones)

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

NOTA:

ISO 27001

EL PROPÓSITO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ES, POR TANTO, GARANTIZAR QUE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN SEAN CONOCIDOS, ASUMIDOS, GESTIONADOS Y MINIMIZADOS POR LA ORGANIZACIÓN DE UNA FORMA DOCUMENTADA, SISTEMÁTICA Y ESTRUCTURADA

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

A continuación, pasamos a desarrollar cada una de estas fases.

1. Análisis y evaluación de riesgos:

Identificación de amenazas, consecuencias y criticidad

Identificación de las amenazas

A continuación, pasamos a desarrollar cada una de estas fases…..

Un SGSI basado en la norma ISO 27001 se fundamenta principalmente en la **identificación y análisis de las principales amenazas** para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos.

FAMILIA ISO 27000

A continuación, pasamos a desarrollar cada una de estas fases.

Una **AMENAZA** se puede definir como **cualquier evento que puede afectar los activos de información** y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser: *ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico.*

En definitiva, se trata de elaborar una adecuada gestión de riesgos que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

A continuación, pasamos a desarrollar cada una de estas fases.

ISO 27001

PARA GARANTIZAR LA CORRECTA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SE DEBEN IDENTIFICAR INICIALMENTE SUS ASPECTOS MÁS RELEVANTES.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

Un correcto proceso de identificación de riesgos implica:

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

FAMILIA ISO 27000

ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS Y SUS CONSECUENCIAS

Se debe **A**nalizar el **I**mpacto en el **N**egocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

BIA= Análisis de Impacto al Negocio

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

Además del riesgo en sí, es necesario analizar también sus CONSECUENCIAS POTENCIALES, que son muchas y de distinta gravedad: **desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales**.

Una posible metodología de evaluación de riesgos estaría compuesta de las siguientes fases:

1) Recogida y preparación de la información.
2) Identificación, clasificación y valoración los grupos de activos.
3) Identificación y clasificación de las amenazas.
4) Identificación y estimación de las vulnerabilidades.
5) Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.
6) Evaluación y análisis del riesgo.

A continuación, pasamos a desarrollar cada una de estas fases.

CRITICIDAD DEL RIESGO

Por este motivo, se deben evaluar las consecuencias potenciales para poder evaluar su criticidad: riesgo aceptable y riesgo residual.

A continuación, pasamos a desarrollar cada una de estas fases.

RIESGO ACEPTABLE

No se trata de eliminar totalmente el riesgo, ya que muchas veces no es posible ni tampoco resultaría rentable, sino de reducir su posibilidad de ocurrencia y minimizar las consecuencias a ***unos niveles que la organización pueda asumir,*** sin que suponga un perjuicio demasiado grave a todos los niveles: económico, logístico, de imagen, de credibilidad, etc.

A continuación, pasamos a desarrollar cada una de estas fases.

ISO 27001

RIESGO RESIDUAL

Se trata del riesgo que permanece y subsiste después de haber implementado los debidos controles, es decir, una vez que la organización haya desarrollado completamente un SGSI. Es un reflejo de las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo inherente.

FAMILIA ISO 27000

A continuación, pasamos a desarrollar cada una de estas fases.

ISO 27001

EL RIESGO RESIDUAL PUEDE ENTENDERSE COMO LO QUE SEPARA A LAS ORGANIZACIONES DE LA SEGURIDAD ABSOLUTA

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

A continuación, pasamos a desarrollar cada una de estas fases.

EL COMPROMISO DEL LIDERAZGO

La norma ISO 27001 otorga un peso cualitativo muy importante a la Dirección, la cual debe ejercer el liderazgo del sistema de seguridad. A partir de aquí, se debe establecer un plan de trabajo en el que quede perfectamente definida la segregación de tareas. Dicho de otro modo: se tiene que establecer con exactitud quién tiene que hacer cada función y cómo ejecutarla.

FAMILIA ISO 27000

LA IMPLEMENTACIÓN DE CONTROLES

Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma ISO 27001 establece en su última versión: ISO/IEC 27001:2013 hasta 113 puntos de control (*en la versión anterior del 2005 eran 133*).

Los 113 controles están divididos por grandes objetivos:

- **Políticas de seguridad de la información.**
- **Controles operacionales.**

Cada empresa, según su parecer, puede añadir más puntos de control si lo considera conveniente, así como personalizarlos para adaptarlos a su propio Plan de Control Operacional, pero siempre deben estar alineados a lo que pide la norma.

Prof: Ing. D. Roca

FORMAS DE AFRONTAR EL RIESGO

Una empresa puede afrontar el riesgo básicamente de tres formas diferentes:

Eliminarlo **Mitigarlo** **O Trasladarlo**

ELIMINAR EL RIEGO

Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, ésta debe poner todos los medios para **tratar de eliminarlo**, de manera que haya un posibilidad cero de que la amenaza se llegue realmente a producir.

MITIGARLO

En la gran mayoría de ocasiones no es posible llegar a la eliminación total del riesgo, ya sea porque es imposible técnicamente o bien porque la empresa decida que no es un riesgo suficientemente crítico. En estos casos la organización puede aceptar el riego, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo.

En definitiva, se trata de implantar las medidas preventivas o correctivas necesarias con el fin de reducir la posibilidad de ocurrencia o el impacto de riesgo.

TRASLADARLO

Esta opción está relacionada con la contratación de **algún tipo de seguro que compense las consecuencias económicas de una pérdida** o deterioro de la información.

Sea cual sea el plan de tratamiento elegido por la empresa, la gestión de riesgos debe garantizar a la organización la tranquilidad de tener suficientemente identificados los riesgos y los controles pertinentes, lo cual le va a permitir actuar con eficacia ante una eventual materialización de los mismos.

En cualquier caso, a la hora de elegir una u otra opción la empresa debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de la información para los procesos de la empresa y el nivel de criticidad del riesgo.

FAMILIA ISO 27000

ISO International Organization for Standardization

UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER CHUQUISACA FUNDADA EN 27 DE MARZO DE 1624

ISO 27001

EL CONCEPTO DE CONTROL EN ESTA NORMA SE DEBE CONSIDERAR COMO UN CONJUNTO DE MEDIDAS, ACCIONES Y/O DOCUMENTOS QUE PERMITEN CUBRIR O AUDITAR CIERTOS RIESGOS

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

5. EL ALCANCE DE LA GESTIÓN

En la planeación para la implementación de un SGSI es muy importante definir el alcance para la implementación del sistema en una organización.

Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar cómo se debe implantar un SGSI.

FAMILIA ISO 27000

ISO International Organization for Standardization

UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER CHUQUISACA FUNDADA EN 27 DE MARZO DE 1624

ISO 27001

NORMALMENTE LA DETERMINACIÓN DEL ALCANCE DE LA GESTIÓN SE REALIZA BIEN POR LÍNEAS DE NEGOCIO O POR MACRO PROCESOS. POR EJEMPLO, SI UNA EMPRESA TIENE DOS LÍNEAS DE NEGOCIO: UNA DE ASESORAMIENTO CONTABLE Y OTRO FISCAL, ES POSIBLE QUE DECIDA PRIORIZAR LA PRIMERA ACTIVIDAD, LA CONTABILIDAD, POR CONSIDERARLA MÁS VULNERABLE EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

6. CONTEXTO DE ORGANIZACIÓN

El análisis de contexto de la organización es fundamental para el SGSI, ya que nos permite determinar los problemas internos y externos de la organización, así como sus debilidades, amenazas, fortalezas y oportunidades que nos puedan afectar.

La norma ISO no especifica el método a utilizar para el análisis del contexto, siendo del método DAFO uno de los más comunes y aceptados. Sea cual sea el sistema elegido, es fundamental someter a valoración tanto el contexto interno (productos y servicios) como externos (logística o clima organizacional).

7. PARTES INTERESADAS

Para poder realizar un correcto análisis de riesgo es preciso definir un contexto de la organización y comprender las necesidades y expectativas de todas las partes interesadas:

- Proveedores de servicios de información y de equipamientos de Tecnologías de la Información (TICs).
- Clientes, poniendo especial cuidado en la gestión de datos de protección personal.
- Fuerzas de seguridad de cada estado y autoridades jurídicas para tratar los aspectos legales.
- Participación en foros profesionales.
- La sociedad en general.

8. FIJACIÓN Y MEDICIÓN DE OBJETIVOS

Fijación de objetivos

Es necesario fijar unos objetivos para la gestión de riegos, los cuales deben poder ser medibles, aunque no es necesario que sean cuantificables.

Otro aspecto básico es que estos objetivos deben ser eficientemente comunicados al conjunto de los empleados de la empresa, puesto que todos los profesionales deben ser conscientes de que participan en un objetivo común, y que un descuido o una mala actitud pueden acarrear consecuencias muy negativas.

ISO 27001

Además, todas las personas que trabajan en la organización deben poseer las competencias necesarias en materia de seguridad de la información según su puesto o función en la empresa.

Por otro lado, cada objetivo definido tiene que estar asociado a unos indicadores que permitan realizar un seguimiento del cumplimiento de las actividades.

9. EL PROCESO DOCUMENTAL

La norma ISO 27001 da mucha importancia a la documentación, estableciendo de manera muy estricta cómo se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para gestionar toda la información. Esta cuestión es fundamental para la obtención de la certificación.

La documentación puede ser presentada en diversos formatos:

Documentos en papel, archivos de texto, hojas de cálculo, archivos de vídeo o audio, etc. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada.

La organización debe gestionar tanto los documentos internos (políticas diversas, procedimientos, documentación del proyecto, etc.), como lo externos (diferentes tipos de correspondencia, documentación recibida con equipamiento, etc.). Por este motivo, la gestión de documentación es una tarea compleja e integral.

Con el objetivo de que las empresas gestionen eficazmente los documentos, la norma ISO 27001 exige la aplicación de un método sistemático para su manejo, así como la redacción de un procedimiento para su gestión.

10. AUDITORÍAS INTERNAS Y REVISIÓN POR LA DIRECCIÓN

LAS AUDITORÍAS INTERNAS

Para garantizar el correcto funcionamiento y mantenimiento de un SGSI basado en la norma ISO 27001, se hace necesario llevar a cabo auditorías internas cada cierto tiempo para poder comprobar que el sistema se encuentra en un estado idóneo.

Existen dos grandes tipos de auditorías internas:

- Gestión. Donde se supervisa el liderazgo, el contexto, etc.
- Controles. En este caso se auditan los 113 controles, normalmente se realiza por personal más experto y puede realizarse en años distintos.

Básicamente, el principal motivo de que se realicen las auditorías internas periódicamente es poder determinar si los procedimientos del SGSI se encuentran conforme a: los requisitos de la norma, la legislación vigente en cada país o sector y los objetivos marcados por la Dirección para el propio sistema de gestión.

FAMILIA ISO 27000

International Organization for Standardization

EL PLAN DE AUDITORÍA INTERNA

ISO 27001

En la planificación de la auditoría se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas. También es necesario definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados.

Si se detectan problemas o desviaciones entre los objetivos de seguridad planteados y los resultados obtenidos, el equipo auditor comprueba si se están aplicando las medidas necesarias, proponiendo nuevas medidas en caso necesario.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

REVISIÓN POR LA DIRECCIÓN

Es fundamental realizar revisiones periódicas del SGSI por parte de la Alta Dirección con el objetivo de comprobar el buen funcionamiento del sistema, si se están cumpliendo los objetivos y también si se está produciendo un Retorno de la Inversión (ROI).

La Alta Dirección de la organización es la máxima responsable de que el área auditada lleve a cabo las acciones necesarias para eliminar las No Conformidades que se hayan detectado durante la auditoría interna

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

Ejemplos de No Conformidades pueden ser: no tener un antivirus instalado en todos los equipos, que el equipo no se encuentre encriptado o que existan contraseñas conocidas por más de una persona, cuando deberían ser unitarias o
individuales.

Durante el seguimiento de las actividades realizadas, se tiene que incluir una verificación de las acciones que se han llevado a cabo, además de un informe en el que se plasmen los resultados obtenidos.