La Auditoría Interna en ISO-27001

SI QUEREMOS TENER UN BUEN SGSI ALINEADO CON LA NORMA ISO 27001, DEBEREMOS TENER EN CUENTA EL PUNTO 6 DE LA MISMA, QUE NOS HABLA DE "AUDITORÍAS INTERNAS DE SGSI"

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

José Luis Martín Martín

CONSULTOR RESPONSABLE DE AUDITORÍA INTERNA

NCS

Introducción

Hemos decidido escribir sobre este tema, pues como dice un viejo refrán: *"las cosas caras vienen en envase chico"*. Y justamente de ello trata el **punto 6** de ISO-27001. Es uno de los más breves de la norma, y sin embargo tal vez sea de los más importantes. Tanto lo es que hasta referencia como nota al pie al estándar ISO-19011, que es la base de referencia más robusta que emplea hoy en día cualquier auditor, y sin embargo, por nuestra experiencia en el tema, podemos afirmar que debe ser uno de los mayores desconocidos (o ausentes) a la hora de aplicar este estándar. Para tratar de ser lo más prácticos posible es por lo que presentamos al principio su base doctrinaria, pero a continuación incluimos lo más "ejemplarmente" posible los pasos que desde NCS solemos dar, para que este artículo pueda ser empleado de forma efectiva.

¿Qué dice la ISO 27001?

Si queremos tener un buen SGSI alineado con la norma ISO 27001, deberemos tener en cuenta el punto 6 de la misma, que nos habla de "Auditorías Internas de SGSI". ¿Y qué nos dice este punto?, pues en primer lugar:

"Obliga a la Organización a realizar auditorías internas a intervalos planificados"

Por lo tanto, para cumplir con lo escrito en la norma, deberemos llevar a cabo **Un Programa de Auditoría** en el que planifiquemos en fechas las mismas y categorías de auditorías a realizar, como veremos más adelante en el Paso 1.

Si continuamos leyendo la norma... *"para determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI están:*

a. Conforme a los requisitos de la ISO 27001

b. Conforme a los requisitos de seguridad de la información identificados

c. Eficazmente implantados y mantenido

d. Se comporta como se espera."

Lo que nos quiere decir, son las comprobaciones a hacer una vez que iniciemos el proceso de auditoría interna, estos serán los objetivos básicos a cumplir.

> El punto 6 de ISO-27001 es uno de los más breves de la norma, y sin embargo tal vez sea de los más importantes

Continuamos con la norma... *Un **programa de auditoría** se debe planificar teniendo en cuenta el estado e importancia de los procesos y las áreas que serán auditados, así como los resultados de las auditorías previas."* Un programa de auditoría no es algo que debamos pasar como "un trámite anual", sino que debemos hacer hincapié en las áreas más sensibles para la organización y por supuesto tener en cuenta las auditorías anteriores con especial atención a las auditorías de

Certificación. No nos debe importar, si las áreas especialmente sensibles deban tener auditorías internas más a menudo.

Si continuamos leyendo… *"Los criterios, el alcance, la frecuencia, y los métodos de auditoría deben ser definidos. La selección de auditores y la dirección de auditoría deben garantizar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo. Las responsabilidades y los requisitos para planificar y dirigir las auditorías, y para informar de los resultados y mantener los registros (véase 4.3.3 Control de Registros) deben estar definidos en un procedimiento documentado."* Todos estos criterios, alcances, métodos, etc., los deberemos contemplar en nuestro **"Procedimiento de Auditoría del Sistema de Información"** donde se definirán todos los puntos necesarios para que las auditorías se ajusten a las necesidades de la organización en imparcialidad, exhaustividad y calidad.

Y para finalizar… *"La dirección responsable del área que está siendo auditada debe asegurar que las acciones para eliminar las no conformidades detectadas y sus causas, se lleven a cabo sin demasiado retraso. El seguimiento de las actividades debe incluir la verificación de las acciones tomadas y el informe de verificación de los resultados"*, lo que la norma nos solicita es que una vez realizada la auditoría, las no conformidades encontradas estén documentadas; en nuestro caso lo veremos en los pasos 7 y 8.

¿Cómo afronta NCS la Auditoría Interna?

A continuación mostraremos una simulación de los pasos que NCS sigue en las Auditorías internas:

Paso 1

Elaborar el Programa Anual de Auditoría Interna teniendo en cuenta a los auditores, tipo de auditoría, y categoría.

Paso 2

Elaborar un Programa Auditor.

Paso 3

Establecer una estructura y lista de verificación para registrar la información o hallazgos encontrados en la auditoría.

El Auditor Jefe comunica con un correo al jefe del Dpto. Auditado el documento (Plantilla del Programa de Auditoría Interna).

Paso 5

Se comunica al departamento a auditar con 10 días hábiles de anticipación el inicio de la Auditoría. El documento "Plantilla de aviso de Auditoría" debe ser firmado por el auditor jefe y por el auditado.

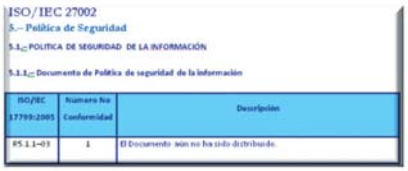
Paso 6

Se presentan las plantillas "de Plan de Auditoría" y "Reunión de Apertura de Cierre"
Se lleva a la auditoría.

Paso 7

Se crea el Informe de auditoría, y se distribuye a todas la áreas implicadas.

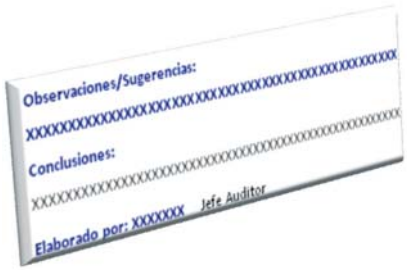
Dividiremos la auditoría en 3 partes, en la primera buscaremos que el SG cumpla con lo establecio en la ISO 27001 e indicamos las No conformidades encontradas con el punto correspondiente a la Norma.



En la segunda parte repasaremos los puntos del Estándar de Seguridad y sus controles basados en la ISO 27002 y comprobaremos su cumplimiento y como en el paso anterior indicaremos las No Conformidades con su punto correspondiente en la Norma.

En la tercera parte examinaremos que cumple con lo escrito en los procedimientos de seguridad y como en los puntos anteriores indicaremos las No Conformidades encontradas y a que Procedimiento de Seguridad corresponden.

La auditoría interna NO debe ser concebida como un acto dedicado a la inspección con tareas a veces incluso policíacas

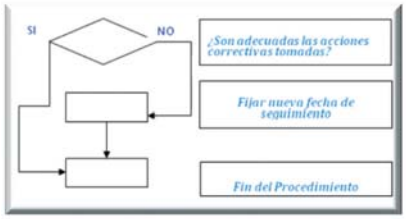


Por último el Jefe Auditor realizará el informe final en el que expondrá las observaciones o sugerencias que considere para mejorar el Sistema y sus conclusiones finales.

Paso 8

En el caso de Existir No Conformidades, el jefe auditor o la persona elegida realizarán el seguimiento de las acciones correctivas y evalúa la eficacia.

Paso 9



Se Comprueba si las acciones correctivas fueron eficaces, aquí puede ocurrir que:
Si el jefe auditor considera que el cierre de las No Conformidades ha sido satisfactorio, dará por concluido el Procedimiento.

Conclusión final:

La auditoría interna NO debe ser concebida como un acto dedicado a la inspección con tareas a veces incluso policíacas en la cual debamos encubrir los delitos ("a ver si no nos pillan"), sino, como una oportunidad de mejora continua con el asesoramiento de los posibles puntos débiles en los cuales se deba hacer hincapié para mejorar la organización.