ISO-27001: LOS CONTROLES (Parte I)

Por: Alejandro Corletti Estrada
Mail: acorletti@hotmail.com

Madrid, noviembre de 2006.

Este artículo es la continuación del análisis de la norma ISO-27001.
Para facilitar su lectura y que no sea tan extenso, se presentará en dos partes. En la presente (Parte I), se desarrollarán los primeros cinco grupos de controles, dejando los seis restantes para la parte II del mismo.

PRÓLOGO

En un artículo anterior a este, denominado "**Análisis de la ISO 27001:2005**", se desarrollaron los conceptos generales de este nuevo estándar de seguridad de la información. Se describió su origen y posicionamiento, y luego se hizo un resumen de las consideraciones clave del mismo. En concreto ese texto presentaba lo siguiente:

> *"Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:*
>
> - ***SGSI (Sistema de Gestión de la Seguridad de la Ingormación o ISMS**: Information Security Managemet System**).***
> - ***Valoración de riegos (Risk Assesment)***
> - ***Controles"***

De esas tres grandes líneas, por ser una presentación de la norma, se continuó con las generalidades y se hizo bastante hincapié en el concepto de SGSI (o ISMS), por considerarse a este tema el que más necesitaba ser explicado inicialmente, pues es lo que verdaderamente hace del estándar un "Sistema completo de Gestión de la Seguridad" (Si bien hay más aspectos que están siendo incorporados en una nueva versión de controles que estará disponible muy brevemente).

Tal vez la conclusión más importante de ese texto fuera que **"Se puede prever, que la certificación ISO-27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo".** Por esta razón es que se consideró necesario seguir adelante con el análisis del mismo.

Los primeros pasos para la implementación de esta norma son:

- Definir el ámbito y política del SGSI.
- Proceso de análisis y valoración de riesgos (Evaluación de Riesgos).
- Selección, tratamiento e implementación de Controles.
- ……

El tercer punto anteriormente presentado es lo que se desarrollará en el presente artículo para tratar de entrar en el detalle de cada uno de los grupos que propone ISO 27001.

DESARROLLO

I. PRESENTACIÓN:

Sobre el tema de Análisis de Riesgo, no se desea profundizar, pues la norma deja abierto el camino a la aplicación de cualquier tipo de metodología, siempre y cuando la misma sea metódica y completa, es decir satisfaga todos los aspectos que se mencionan en ella. Existen varios tipos de metodologías, en España las más empleadas, tal vez sean MAGERIT y COBIT, pero hasta es posible la aplicación de procedimientos propietarios o particulares, si presenta rigurosidad en los pasos y resultados.

Lo que es necesario recalcar aquí es que los controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo. Es decir, que de esta actividad surgirá la primera decisión acerca de los controles que se deberán abordar.

La preparación y planificación de SGSI, se trató en el artículo anterior, pero en definitiva, lo importante de todo este proceso es que desencadena en una serie de **controles** (o mediciones) a considerar y documentar, que se puede afirmar, **son uno de los aspectos fundamentales del SGSI** (junto con la Valoración de riesgo). Cada uno de ellos se encuentra en estrecha relación a todo lo que especifica la norma ISO/IEC 17799:2005 en los puntos 5 al 15, y tal vez estos sean el máximo detalle de afinidad entre ambos estándares. La evaluación de cada uno de ellos debe quedar claramente documentada, y muy especialmente la de los controles que se consideren excluidos de la misma.

"DESCONCEPTO": Al escuchar la palabra "**Control**", automáticamente viene a la mente la idea de alarma, hito, evento, medición, monitorización, etc…., se piensa en algo muy **técnico o acción**. En el caso de este estándar, el concepto de "**Control**", **es mucho** (pero mucho) **más que eso**, pues abarca todo el conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas, etc…….

Un "**Control**" es lo que permite garantizar que cada aspecto,
que se valoró con un cierto riesgo, queda cubierto y auditable
¿Cómo? → De muchas formas posibles.

El estándar especifica en su "Anexo A" el listado completo de cada uno de ellos, agrupándolos en once rubros. Para cada uno de ellos define el objetivo y lo describe brevemente.

Cabe aclarar que el anexo A proporciona una buena base de referencia, no siendo exhaustivo, por lo tanto se pueden seleccionar más aún. Es decir, estos 133 controles (hoy) son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control. Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentará huecos claramente identificables.

Los controles que el anexo A de esta norma propone quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad
A.6 Organización de la información de seguridad
A.7 Administración de recursos
A.8 Seguridad de los recursos humanos
A.9 Seguridad física y del entorno
A.10 Administración de las comunicaciones y operaciones
A.11 Control de accesos
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
A.13 Administración de los incidentes de seguridad
A.14 Administración de la continuidad de negocio
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

II. DESARROLLO DE LOS CONTROLES

En este ítem, para ser más claro, se respetará la puntuación que la norma le asigna a cada uno de los controles.

A.5 Política de seguridad.

Este grupo está constituido por dos controles y es justamente el primer caso que se puede poner de manifiesto sobre el mencionado "Desconcepto" sobre lo que uno piensa que es un control, pues aquí se puede apreciar claramente la complejidad que representa el diseño, planificación, preparación, implementación y revisiones de una Política de Seguridad (la revisión es justamente el segundo control que propone)…….como se mencionó *"un Control es mucho (pero mucho), mas que eso…"*

Todo aquel que haya sido responsable alguna vez de esta tarea, sabrá de lo que se está hablando. La Política de Seguridad, para ser riguroso, en realidad debería dividirse en dos documentos:

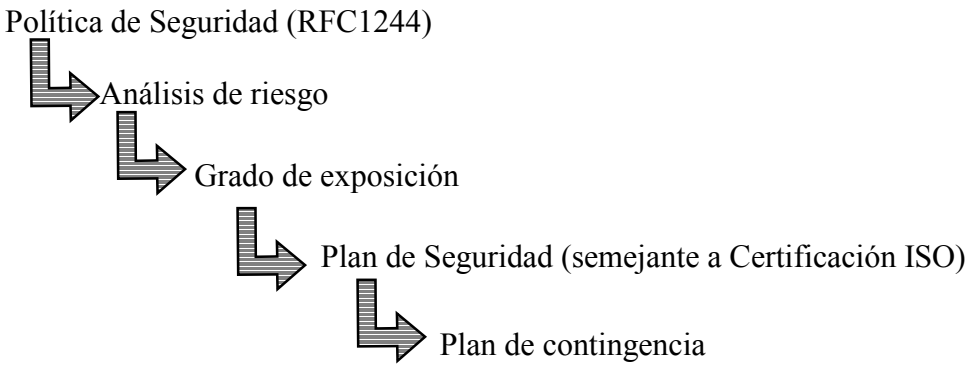
- Política de seguridad (Nivel político o estratégico de la organización): Es la mayor línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.
- Plan de Seguridad (Nivel de planeamiento o táctico): Define el "Cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

Algo sobre lo que generalmente no se suele reflexionar o remarcar es que:

Una "Política de Seguridad" bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.

Haciendo abuso de la avanzada edad de este autor, es que se van a citar dos puntos de partida para la mencionada actividad que, a juicio del mismo, siguen siendo grandes referentes metodológicos a la hora de la confección de estos controles.

Se trata de lo que proponen las siguientes RFCs (Request For Comments). Política de seguridad (**RFC – 2196** Site Security Handbook) y también la anterior (**RFC-1244**, que si bien queda obsoleta por la primera es muy ilustrativa) ambas, planten una metodología muy eficiente de feedback partiendo desde el plano más alto de la Organización hasta llegar al nivel de detalle, para comparar nuevamente las decisiones tomadas y reingresar las conclusiones al sistema evaluando los resultados y modificando las deficiencias. Se trata de un ciclo permanente y sin fin cuya característica fundamental es la constancia y la actualización de conocimientos. Esta recomendación plantea muy en grande los siguientes pasos:



La política es el marco estratégico de la Organización, es el más alto nivel. El análisis de riesgo y el grado de exposición determinan el impacto que puede producir los distintos niveles de clasificación de la información que se posee. Una vez determinado estos conceptos, se pasa al Cómo que es el Plan de Seguridad, el cual, si bien en esta RFC no está directamente relacionado con las normas ISO, se mencionan en este texto por la similitud en la elaboración de procedimientos de detalle para cada actividad que se implementa, y porque se reitera, su metodología se aprecia como excelente……*(y dados los años del autor, sabrán disculpar la fechas de publicación de ambas RFCs....*{Les garantizo que están en Inglés, y no en Sánscrito}*)*.

A.6 Organización de la información de seguridad.

Este segundo grupo de controles abarca once de ellos y se subdivide en:

- Organización Interna: Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.
- Partes externas: Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.

Lo más importante a destacar de este grupo son dos cosas fundamentales que abarcan a ambos subgrupos:

- Organizar y Mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (Personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc.).
- Derechos y obligaciones de cualquiera de los involucrados.

En este grupo de controles, lo ideal es diseñar e implementar una simple base de datos, que permita de forma amigable, el alta, baja y/o modificación de cualquiera de estos campos. La redacción de la documentación inicial de responsables: derechos y obligaciones (para personal interno y ajeno) y el conjunto de medidas a adoptar con cada uno de ellos. Una vez lanzado este punto de partida, se debe documentar la metodología de actualización, auditabilidad y periodicidad de informes de la misma.

A.7 Administración de recursos

Este grupo cubre cinco controles y también se encuentra subdividido en:

- Responsabilidad en los recursos: Inventario y propietario de los recursos, empleo aceptable de los mismos.
- Clasificación de la información: Guías de clasificación y Denominación, identificación y tratamiento de la información.

Este grupo es eminentemente procedimental y no aporta nada al aspecto ya conocido en seguridad de la información, en cuanto a que todo recurso debe estar perfectamente inventariado con el máximo detalle posible, que se debe documentar el "uso adecuado de los recursos" y que toda la información deberá ser tratada de acuerdo a su nivel. En el caso de España, tanto la LOPD como la LSSI han aportado bastante a que esta tarea sea efectuada con mayor responsabilidad en los últimos años. También se puede encontrar en Internet varias referencias a la clasificación de la información por niveles.

Tal vez sí valga la pena mencionar aquí el problema que se suele encontrar en la gran mayoría de las empresas que cuentan con un parque informático considerable, sobre el cual, se les dificulta

mucho el poder mantener actualizado su sistema de inventario. El primer comentario, es que este aspecto debe abordarse "**sí o sí**", pues es imposible pensar en seguridad, si no se sabe fehacientemente lo que se posee y cada elemento que queda desactualizado o no se lo ha inventariado aún, es un **hueco concreto en la seguridad de todo el sistema**, y de hecho suelen ser las mayores y más frecuentes puertas de entrada, pues están al margen de la infraestructura de seguridad .

El segundo comentario, es que se aprecia que las mejores metodologías a seguir para esta actividad, son las que permiten **mantener "vivo"** el estado de la red y por medio de ellas inventariar lo que se "escucha". Esta metodología lo que propone es, hacer un empleo lógico y completo de los elementos de red o seguridad (IDSs, Firewalls, Routers, sniffers, etc.) y aprovechar su actividad cotidiana de escucha y tratamiento de tramas para mantener "vivo" el estado de la red. Es decir, nadie mejor que ellos saben qué direcciones de la "Home Net" se encuentran activas y cuáles no, por lo tanto, aprovechar esta funcionalidad para almacenar y enviar estos datos a un repositorio adecuado, el cual será el responsable de mantener el inventario correspondiente. Sobre este tema, se propone la lectura de dos artículos publicados hace tiempo en Internet por este autor que se denominan "**Metodología Nessus-Snort**" y "**Matriz de Estado de Seguridad**", si bien los mismos deben ser actualizados al día de hoy, de ellos se puede obtener una clara imagen de cómo se puede realizar esta tarea y aprovechar las acciones de seguridad para mejorar el análisis de riesgo y el inventario.

A.8 Seguridad de los recursos humanos.

Este grupo cubre nueve controles y también se encuentra subdividido en:

- Antes del empleo: Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.
- Durante el empleo: Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.
- Finalización o cambio de empleo: Finalización de responsabilidades, devolución de recursos, revocación de derechos.

Este grupo, en la actualidad, debe ser el gran ausente en la mayoría de las organizaciones. Se trata de un serio trabajo a realizar entre RRHH y los responsables de Seguridad de la Información de la organización.

Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido). En la misma deberá quedar bien claro las acciones a seguir para los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información que tenga ese puesto. Como se pueda apreciar, tanto la contratación como el cese de un puesto, es una actividad conjunta de estas dos áreas, y cada paso deberá ser coordinado, según la documentación confeccionada, para que no se pueda pasar por alto ningún detalle, pues son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido, mantiene accesos o permisos que no se debieran (casos muy comunes).

Tanto el inicio como el cese de cualquier tipo de actividad relacionada con personal responsable de manejo de información de la organización, **son actividades muy fáciles de procedimentar**, pues no dejan de ser un conjunto de acciones secuenciales muy conocidas que se deben seguir "a raja tabla" y que paso a paso deben ser realizadas y controladas……..se trata simplemente de ¡¡¡ESCRIBIRLO!!! (y por supuesto de cumplirlo luego), esto forma parte de las pequeñas cosas que cuestan poco y valen mucho ¿Por qué será que no se hacen????

En cuanto a formación, para dar cumplimiento al estándar, no solo es necesario dar cursos. Hace falta contar con un "Plan de formación". La formación en seguridad de la información, no puede ser una actividad aperiódica y determinada por el deseo o el dinero en un momento dado, tiene que ser tratada como cualquier otra actividad de la organización, es decir se debe plantear:

- Meta a la que se desea llegar.
- Determinación de los diferentes perfiles de conocimiento.
- Forma de acceder al conocimiento.
- Objetivos de la formación.
- Metodología a seguir.
- Planificación y asignación de recursos.
- Confección del plan de formación.
- Implementación del plan.
- Medición de resultados.
- Mejoras.

Si se siguen estos pasos, se llegará a la meta, pero no solo a través de la impartición de uno o varios cursos o la distribución de documentos de obligada lectura, sino con un conjunto de acciones que hará que se complementen e integren en todo el SGSI como una parte más, generando concienciación y adhesión con el mismo.

A.9 Seguridad física y del entorno

Este grupo cubre trece controles y también se encuentra subdividido en:

- Áreas de seguridad: Seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas e seguridad, accesos públicos, áreas de entrega y carga.
- Seguridad de elementos: Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

A juicio del autor, uno de los mejores resultados que se pueden obtener en la organización de una infraestructura de seguridad de la información, está en plantearla siempre por niveles. Tal vez no sea necesario hacerlo con el detalle de los siete niveles del modelo ISO/OSI, pero sí por lo menos de acuerdo al modelo TCP/IP que algunos consideran de cuatro (Integrando físico y enlace) y otros de cinco niveles.

Nuevamente el criterio de este autor, aprecia que es correcto considerar separadamente el nivel físico con el de enlace, pues presentan vulnerabilidades muy diferentes. Si se presenta entonces el modelo de cinco niveles, se puede organizar una estructura de seguridad contemplando medidas y acciones por cada uno de ellos, dentro de las cuales se puede plantear, por ejemplo, lo siguiente:

- **Aplicación:** Todo tipo de aplicaciones.
- **Transporte:** Control de puertos UDP y TCP.
- **Red:** Medidas a nivel protocolo IP e ICMP, túneles de nivel 3.
- **Enlace:** Medidas de segmentación a nivel direccionamiento MAC, tablas estáticas y fijas en switchs, control de ataques ARP, control de broadcast y multicast a nivel enlace, en el caso WiFi: verificación y control de enlace y puntos de acceso, 802.X (Varios), empleo de túneles de nivel 2, etc.
- **Físico:** Instalaciones, locales, seguridad perimetral, CPDs, gabinetes de comunicaciones, control de acceso físico, conductos de comunicaciones, cables, fibras ópticas, radio enlaces, centrales telefónicas (Tema a desarrollar en este punto)

Como se puede apreciar, este es una buena línea de pensamiento para plantear cada una de las actividades y evitar que se solapen algunas de ellas y/o que queden brechas de seguridad.

En el caso físico, es conveniente también separar todas ellas, por lo menos en los siguientes documentos:

- Documentación de control de accesos y seguridad perimetral general, áreas de acceso y entrega de materiales y documentación, zonas públicas, internas y restringidas, responsabilidades y obligaciones del personal de seguridad física.
- Documentación de CPDs: Parámetros de diseño estándar de un CPD, medidas de protección y alarmas contra incendios/humo, caídas de tensión, inundaciones, control de climatización (Refrigeración y ventilación), sistemas vigilancia y control de accesos, limpieza, etc.
- Documentación y planos de instalaciones, canales de comunicaciones, cableado, enlaces de radio, ópticos u otros, antenas, certificación de los mismos, etc.
- Empleo correcto del material informático y de comunicaciones a nivel físico: Se debe desarrollar aquí cuales son las medidas de seguridad física que se debe tener en cuenta sobre los mismos (Ubicación, acceso al mismo, tensión eléctrica, conexiones físicas y hardware permitido y prohibido, manipulación de elementos, etc.) . No se incluye aquí lo referido a seguridad lógica.
- Seguridad física en el almacenamiento y transporte de material informático y de comunicaciones: Zonas y medidas de almacenamiento, metodología a seguir para el ingreso y egreso de este material, consideraciones particulares para el transporte del mismo (dentro y fuera de al organización), personal autorizado a recibir, entregar o sacar material, medidas de control. No se incluye aquí lo referido a resguardo y

recuperación de información que es motivo de otro tipo de procedimientos y normativa.

- Documentación de baja, redistribución o recalificación de elementos: Procedimientos y conjunto de medidas a seguir ante cualquier cambio en el estado de un elemento de Hardware (Reubicación, cambio de rol, venta, alquiler, baja, destrucción, compartición con terceros, incorporación de nuevos módulos, etc.).

III. RESUMEN y CONCLUSIONES PARCIALES DE ESTA PARTE.

- Como se pudo apreciar hasta ahora, el concepto de "Control", no es el convencional que se puede tener al respecto. Se lo debe considerar como un conjunto de medidas, acciones y/o documentos que permiten cubrir y auditar cierto riesgo.

- Una "Política de Seguridad" bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI. Es recomendable subdividirla en un Plan y en una Política de seguridad (Consejo "*de viejo"*: Ver RFCs: 1244 y 2196)

- Organizar: Responsables, obligaciones, derechos, acuerdos, etc (Base de datos y documentación que la sustente).

- Recursos: Responsables de los mismos y clasificación de la información que contienen. LOPD, LSSI. Inventario "VIVO" (Consejo: aprovechar al máximo los elementos de Red y Seguridad, *para eso están*).

- Recursos humanos: Coordinar y sincronizar el trabajo de ambas gerencias (RRHH y Seguridad). Tres momentos fundamentales: Inicio – durante (Plan de formación) – Cese. Documentar y procedimentar los pasos que "tácitamente" se siguen.

- Seguridad física: Mentalidad de "Niveles TCP/IP" para dividir bien las tareas.

Alejandro Corletti Estrada, Madrid, noviembre de 2006.