ISO-27001: LOS CONTROLES (Parte II)

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

Madrid, "Navidad" 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 presentó en dos partes.
A principios del mes de noviembre se publicó la primera parte, denominada: *"ISO-27001: Los Controles (Parte I)"*, en la cual se desarrollaron los primeros cinco grupos de controles, dejando los seis restantes para este último texto, denominado parte II, con el cual completa la totalidad de los once controles que propone este estándar.

PRÓLOGO

Como se acaba de mencionar, para un entendimiento más completo del enunciado y objetivo de este estándar, se aconseja realizar una lectura previa de los dos artículos anteriores:

- "**Análisis de la ISO 27001:2005**"
- **"ISO-27001: Los Controles (Parte I)"**

En los mismos se realiza una presentación del estándar y luego se desarrollan los primeros cinco controles, de los once que propone esta norma.

Durante este texto se tratarán de resumir los aspectos fundamentales que cubren el resto de los controles, para poder obtener como resultado una visión completa de lo que debe ser considerado en cualquier organización que desee preparar e implementar un verdadero Sistema de Gestión de la Seguridad de la Información (**SGSI**), y de esta forma preparar el camino para una certificación en el estándar ISO 27001, que como ya se mencionó en los artículos anteriores, se aprecia, será uno de los pilares fundamentales para definir la "Calidad" con que se adoptan y gestionan acciones y medidas de seguridad sobre los recursos de una empresa.

Los controles que se tratarán en este texto son (respetando la numeración que les asigna el Anexo A del estándar):

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 Marco legal y buenas prácticas

DESARROLLO

I. PRESENTACIÓN:

En virtud de tratarse de una continuación, se presupone que se ha leído la parte precedente a este texto, por lo tanto no es necesario reiterar las ideas básicas que comprende la presentación de un tema.

En esta caso sólo se desea incidir una vez más sobre el **"DESCONCEPTO"** de Control, pues 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.

Volviendo a los controles que el anexo A de esta norma propone, se han desarrollado ya:

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

Quedando para el presente texto entonces:

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 Marco legal y buenas prácticas

Que se desarrollan a continuación.

II. DESARROLLO DE LOS CONTROLES

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

A.10 Administración de las comunicaciones y operaciones

Este grupo comprende treinta y dos controles, es el más extenso de todos y se divide en:

- Procedimientos operacionales y responsabilidades: Tiene como objetivo asegurar la correcta y segura operación de la información, comprende cuatro controles. Hace especial hincapié en documentar todos los procedimientos, manteniendo los mismos y disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos.

  Esta tarea en todas las actividades de seguridad (no solo informática), se suele realizar por medio de lo que se denomina Procedimientos Operativos Normales (PON) o Procedimientos Operativos de Seguridad (POS), y en definitiva consiste en la realización de documentos breves y ágiles, que dejen por sentado la secuencia de pasos o tareas a llevar a cabo para una determinada función. Cuanto mayor sea el nivel de desagregación de esta función, más breve será cada PON (también habrá mayor cantidad de ellos) y a su vez más sencillo y comprensible. Luego de trabajar algún tiempo en esta actividad, se llegará a comprender que la mayoría de las actividades relacionadas con seguridad, son fácilmente descriptibles, pues suelen ser una secuencia de pasos bastante "mecanizables", y allí radica la importancia de estos procedimientos. La enorme ventaja que ofrece poseer todo procedimentado es:

  - Identificar con absoluta claridad los responsables y sus funciones.
  - Evitar la "imprescindibilidad" de ciertos administradores.
  - Evitar ambigüedades el procedimientos.
  - Detectar "zonas grises" o ausencias procedimentales (futuras brechas de seguridad).

- Administración de prestación de servicios de terceras partes: Abarca tres controles, se refiere fundamentalmente, como su nombre lo indica, a los casos en los cuales se encuentran tercerizadas determinadas tareas o servicios del propio sistema informático. Los controles están centrados en tres aspectos fundamentales de esta actividad:

  - Documentar adecuadamente los servicios que se están prestando (acuerdos, obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).
  - Medidas a adoptar para la revisión, monitorización y auditoría de los mismos
  - Documentación adecuada que permita regularizar y mantener un eficiente control de cambios en estos servicios.

- Planificación y aceptación de sistemas: El objetivo es realizar una adecuada metodología para que al entrar en producción cualquier sistema, se pueda minimizar el riesgo de fallos. De acuerdo a la magnitud de la empresa y al impacto del sistema a considerar, siempre es

una muy buena medida la realización de maquetas. Estas maquetas deberían "acercarse" todo lo posible al entorno en producción, para que sus pruebas de funcionamiento sean lo más veraces posibles, simulando ambientes de trabajo lo más parecidos al futuro de ese sistema (Hardware y Software, red, carga de operaciones y transacciones, etc.), cuanto mejor calidad y tiempo se dedique a estas maquetas, menor será la probabilidad de fallos posteriores, es una relación inversamente proporcional que se cumple en la inmensa mayoría de los casos.

Los dos aspectos claves de este control son el diseño, planificación, prueba y adecuación de un sistema por un lado; y el segundo, es desarrollar detallados criterios de aceptación de nuevos sistemas, actualizaciones y versiones que deban ser implantados. Este último aspecto será un documento muy "vivo", que se realimentará constantemente en virtud de las modificaciones, pruebas, incorporaciones y avances tecnológicos, por lo tanto se deberá confeccionar de forma flexible y abierto a permanentes cambios y modificaciones.

- Protección contra código móvil y maligno: el objetivo de este apartado es la protección de la integridad del software y la información almacenada en los sistemas.

  El código móvil es aquel que se transfiere de un equipo a otro para ser ejecutado en el destino final, este empleo es muy común en las arquitecturas cliente-servidor, y se está haciendo más común en las arquitecturas "víctima-gusano", por supuesto con un empleo no tan deseado. Sobre el empleo seguro de Código móvil, recomiendo que el que esté interesado, profundice en una metodología que esta haciendo las cosas bien, que se denomina "**Proof-Carring Code**" (**PCC**), la cual propone la implementación de medidas para garantizar que los programas que serán ejecutados en el cliente lo hagan de forma segura. Se puede encontrar mucha información al respecto en Internet.

  En cuanto al código malicioso, a esta altura no es necesario ahondar en ningún detalle al respecto, pues "quien esté libre de virus y troyanos que tire la primera piedra". El estándar hace referencia al conjunto de medidas comunes que ya suelen ser aplicadas en la mayoría de las empresas, es decir, detección, prevención y recuperación de la información ante cualquier tipo de virus. Tal vez lo más importante aquí y suele ser el punto débil de la gran mayoría es la preparación y la existencia de procedimientos (Lo que implica practicarlos). En mi opinión es donde más frecuentemente se encuentran fallos. **La gran mayoría de las empresas confían su seguridad antivirus en la mera aplicación de un determinado producto y nada más**, pero olvidan preparar al personal de administradores y usuarios en cómo proceder ante virus y, por supuesto, tampoco realizan procedimientos de recuperación y verificación del buen funcionamiento de lo documentado (si es que lo tienen…..). Esto último, es una de las primeras y más comunes objeciones que aparecen al solicitar certificaciones en estos estándares. Lo recalco una vez más, no es eficiente el mejor producto antivirus del mercado, sino se realizan estas dos últimas tareas que se han mencionado: Preparación del personal e implementación (con prácticas) de procedimientos.

- Resguardo: El objetivo de esta apartado conceptualmente es muy similar al anterior, comprende un solo control que remarca la necesidad de las copias de respaldo y recuperación. Siguiendo la misma insistencia del párrafo precedente, de nada sirve realizar copias de respaldo y recuperación, sino se prepara al personal e implementan las mismas con prácticas y procedimientos

- Administración de la seguridad de redes: Los dos controles que conforman este apartado hacen hincapié en la necesidad de administrar y controlar lo que sucede en nuestra red, es decir, implementar todas las medidas posibles para evitar amenazas, manteniendo la seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella. Se deben implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece, tanto propios como tercerizados.

- Manejo de medios: En esta traducción, como "medio" debe entenderse todo elemento capaz de almacenar información (discos, cintas, papeles, etc. tanto fijos como removibles). Por lo tanto el objetivo de este grupo es, a través de sus cuatro controles, prevenir la difusión, modificación, borrado o destrucción de cualquiera de ellos o lo que en ellos se guarda.

  En estos párrafos describe brevemente las medidas a considerar para administrar medios fijos y removibles, su almacenamiento seguro y también por períodos prolongados, evitar el uso incorrecto de los mismos y un control específico para la documentación.

  De todo ello, lo que debe rescatarse especialmente, es el planteo de este problema de los medios, procedimentarlo, practicarlo y mejorarlo con la mayor frecuencia que se pueda.

- Intercambios de información: Este grupo contempla el conjunto de medidas a considerar para cualquier tipo de intercambio de información, tanto en línea como fuera de ella, y para movimientos internos o externos de la organización.

  Aunque a primera vista no lo parezca, son muchos los aspectos que deben ser tenidos en cuenta para esta tarea. No debe olvidarse que la información es **el bien más preciado de una empresa, por lo tanto al igual que en un Banco, cuando la misma se mueve, no es nada más ni nada menos que un "desplazamiento de caudales"**, es decir con todas las prevenciones, vigilancias, procesos, agentes especializados/entrenados y…… hasta con camión blindado. Los aspectos que no se pueden dejar librados al azar son:

  - Políticas, procedimientos y controles para el intercambio de información para tipo y medio de comunicación a emplear.
  - Acuerdos, funciones, obligaciones, responsabilidades y sanciones de todas las partes intervinientes.
  - Medidas de protección física de la información en tránsito.
  - Consideraciones para los casos de mensajería electrónica
  - Medidas particulares a implementar para los intercambios de información de negocio, en especial con otras empresas.

- Servicios de comercio electrónico: Este grupo, supone que la empresa sea la prestadora de servicios de comercio electrónico, es decir, no aplica a que los empleados realicen una transacción, por parte de la empresa o por cuenta propia, con un servidor ajeno a la misma.

  La prestación de servicios de comercio electrónico por parte de una empresa exige el cumplimiento de varios detalles desde el punto de vista de la seguridad:

  - Metodologías seguras de pago.
  - Confidencialidad e integridad de la transacción.
  - Mecanismos de no repudio.

- Garantías de transacción.
- Conformidades legales, desde el punto de vista de LSSI y LOPD (en España), como así también del código de Comercio.

Para el cumplimiento de lo expuesto es que este grupo presenta, a través de tres controles, un conjunto de medidas a considerar referidas al control de información que circula a través de redes públicas para evitar actividades fraudulentas, difusión, modificación o mal uso de la misma. Medidas tendientes a evitar transacciones incompletas, duplicaciones o réplicas de las mismas, y por último mecanismos que aseguren la integridad de la totalidad de la información disponible.

- Monitorización: Este apartado tiene como objetivo la detección de actividades no autorizadas en la red y reúne seis controles. Los aspectos más importantes a destacar son:
  - Auditar Logs que registren actividad, excepciones y eventos de seguridad.
  - Realizar revisiones periódicas y procedimientos de monitorización del uso de los sistemas.
  - Implementación de robustas medidas de protección de los Logs de información de seguridad. Se debe considerar que una de las primeras enseñanzas que recibe cualquier aprendiz de intruso, es a borrar sus huellas para poder seguir operando sin ser descubierto el mayor tiempo posible. Por esta razón, es una de las principales tareas de seguridad, la de proteger todo indicio o prueba de actividad sospechosa. En casos de máxima seguridad, se llega hasta el extremo de tener una impresora en línea, que va registrando sobre papel en tiempo real, cada uno de los logs que se configuran como críticos, pues es uno de los pocos medios que no puede ser borrado remotamente una vez detectada la actividad. También como experiencia personal, he llegado a ver realizar la misma actividad en CDs de una sola escritura.
  - La actividad de los administradores y operadores de sistemas, también debe ser monitorizada, pues es una de las mejores formas de tomar conocimiento de actividad sospechosa, tanto si la hace un administrador propio de la empresa (con o sin mala intención) o si es uno que se hace pasar por uno de ellos. Hay que destacar que una vez que se posee acceso a una cuenta de administración, se tiene control total de esa máquina y en la mayoría de los casos, ya está la puerta abierta para el resto de la infraestructura, es decir, se emplea es máquina como puente o máquina de salto hacia las demás.
  - Así como es vital, ser estricto con el control de Logs, lo es también el saber lo antes posible, si cualquiera de ellos está fallando, pues esa debe ser la segunda lección de un aprendiz de intruso. Es decir, lograr que se dejen de generar eventos de seguridad por cada paso que da. Por lo tanto, es necesario implementar un sistema de alarmas que monitorice el normal funcionamiento de los sistemas de generación de eventos de seguridad y/o Logs.
  - Sincronización de tiempos: Hoy en día el protocolo NTP (Network Time Protocol) está tan difundido y fácilmente aplicable que es un desperdicio no usarlo. Se debe implementar una buena estrategia de estratos, tal cual lo propone este protocolo, y

sincronizar toda la infraestructura de servidores, tanto si se depende de ellos para el funcionamiento de los servicios de la empresa, como si no. Pues cuando llega la hora de investigar, monitorizar o seguir cualquier actividad sospechosa es fundamental tener una secuencia cronológica lógica que permita moverse pro todos los sistemas de forma coherente. De acuerdo a la actividad de la empresa, se deberá ser más o menos estrictos con la precisión del reloj del máximo estrato (hacia el exterior) el cual puede soportar mayor flexibilidad en los casos que no sea vital su exactitud con las jerarquías internacionales y luego el resto de las máquinas dependerán de este. Pero lo que no debe suceder y así lo exige esta norma, es la presencia de servidores que no estén sincronizados.

A.11 Control de accesos

No se debe confundir la actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente "sea, quien dice ser". El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:

- Encauzar (o enjaular) al usuario debidamente.
- Verificar el desvío de cualquier acceso, fuera de lo correcto.

El control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Al igual que sucede en el mundo de la seguridad física, cualquiera que ha tenido que acceder a una caja de seguridad bancaria vivió como a medida que uno de llegando a áreas de mayor criticidad, las medidas de control de acceso se incrementan, en un sistema informático debería ser igual.

Para cumplir con este propósito, este apartado lo hace a través de veinticinco controles, que los agrupa de la siguiente forma:

- Requerimientos de negocio para el control de accesos: Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.
- Administración de accesos de usuarios: Tiene como objetivo asegurar el correcto acceso y prevenir el no autorizado y, a través de cuatro controles, exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la organización.
- Responsabilidades de usuarios: Todo usuario dentro de la organización debe tener documentadas sus obligaciones dentro de la seguridad de la información de la empresa. Independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información. Evidentemente existirán diferentes grados de responsabilidad, y proporcionalmente a ello, las obligaciones derivadas de estas funciones. Lo que **no** puede suceder es que algún usuario las desconozca. Como ningún ciudadano

desconoce por ejemplo, las medidas de seguridad vial, pues el tráfico sería caótico (¿más aún????), de igual forma no es admisible que el personal de la empresa no sepa cuál es su grado de responsabilidad en el manejo de la información de su nivel. Por lo tanto de este ítem se derivan tres actividades.

- Identificar niveles y responsabilidades.
- Documentarlas correctamente.
- Difundirlas y verificar su adecuada comprensión.

Para estas actividades propone tres controles, orientados a que los usuarios deberán aplicar un correcto uso de las contraseñas, ser conscientes del equipamiento desatendido (por lugar, horario, lapsos de tiempo, etc.) y de las medidas fundamentales de cuidado y protección de la información en sus escritorios, medios removibles y pantallas.

- Control de acceso a redes: Todos los servicios de red deben ser susceptibles de medidas de control de acceso; para ello a través de siete controles, en este grupo se busca prevenir cualquier acceso no autorizado a los mismos.

  Como primer medida establece que debe existir una política de uso de los servicios de red para que los usuarios, solo puedan acceder a los servicios específicamente autorizados. Luego se centra en el control de los accesos remotos a la organización, sobre los cuales deben existir medidas apropiadas de autenticación.

  Un punto sobre el que merece la pena detenerse es sobre la identificación de equipamiento y de puertos de acceso. Este aspecto es una de las principales medidas de control de seguridad. En la actualidad se poseen todas las herramientas necesarias para identificar con enorme certeza las direcciones, puertos y equipos que pueden o no ser considerados como seguros para acceder a las diferentes zonas de la empresa. Tanto desde una red externa como desde segmentos de la propia organización. En los controles de este grupo menciona medidas automáticas, segmentación, diagnóstico y control equipamiento, direcciones y de puertos, control de conexiones y rutas de red. Para toda esta actividad se deben implementar: IDSs, IPSs, FWs con control de estados, honey pots, listas de control de acceso, certificados digitales, protocolos seguros, túneles, etc… Es decir, existen hoy en día muchas herramientas para implementar estos controles de la mejor forma y eficientemente, por ello, tal vez este sea uno de los grupos que más exigencia técnica tiene dentro de este estándar.

- Control de acceso a sistemas operativos: El acceso no autorizado a nivel sistema operativo presupone uno de los mejores puntos de escalada para una intrusión; de hecho son los primeros pasos de esta actividad, denominados "*Fingerprintig y footprinting*", pues una vez identificados los sistemas operativos, versiones y parches, se comienza por el más débil y con solo conseguir un acceso de usuario, se puede ir escalando en privilegios hasta llegar a encontrar el de "*root*", con lo cual ya no hay más que hablar. La gran ventaja que posee un administrador, es que las actividades sobre un sistema operativo son mínimas, poco frecuentes sus cambios, y desde ya que no comunes a nivel usuario del sistema, por lo tanto si se saben emplear las medidas adecuadas, se puede identificar rápidamente cuando la actividad es sospechosa, y en definitiva es lo que se propone en este grupo: Seguridad en la validación de usuarios del sistema operativo, empleo de identificadores únicos de usuarios, correcta administración de contraseñas, control y limitación de tiempos en las sesiones y por último

verificaciones de empleo de utilidades de los sistemas operativos que permitan realizar acciones "interesantes".

- Control de acceso a información y aplicaciones: En este grupo, los dos controles que posee están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura. Este último proceder es muy común en sistemas críticos (Salas de terapia intensiva, centrales nucleares, servidores primarios de claves, sistemas de aeropuertos, militares, etc.), los cuales no pueden ser accedidos de ninguna forma vía red, sino únicamente estando físicamente en ese lugar. Por lo tanto si se posee alguna aplicación que entre dentro de estas consideraciones, debe ser evaluada la necesidad de mantenerla o no en red con el resto de la infraestructura.
- Movilidad y teletrabajo: Esta nueva estructura laboral, se está haciendo cotidiana en las organizaciones y presenta una serie de problemas desde el punto de vista de la seguridad:
    - Accesos desde un ordenador de la empresa, personal o público.
    - Posibilidades de instalar o no, medidas de hardware/software seguro en el ordenador remoto.
    - Canales de comunicaciones por los cuales se accede (red publica, privada, GPRS, UMTS, WiFi, Túnel, etc.).
    - Contratos que se posean sobre estos canales.
    - Personal que accede: propio, tercerizado, o ajeno.
    - Lugar remoto: fijo o variable.
    - Aplicaciones e información a la que accede.
    - Nivel de profundidad en las zonas de red a los que debe acceder.
    - Volumen y tipo de información que envía y recibe.
    - Nivel de riesgo que se debe asumir en cada acceso.

    Cada uno de los aspectos expuestos merece un tratamiento detallado y metodológico, para que no surjan nuevos puntos débiles en la estructura de seguridad.

    La norma no entra en mayores detalles, pero de los dos controles que propone se puede identificar que la solución a esto es adoptar una serie de procedimientos que permitan evaluar, implementar y controlar adecuadamente estos aspectos en el caso de poseer accesos desde ordenadores móviles y/o teletrabajo.

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

Este grupo reúne dieciseis controles.

- Requerimientos de seguridad de los sistemas de información: Este primer grupo que incluye un solo control, plantea la necesidad de realizar un análisis de los requerimientos que deben

exigirse a los sistemas de información, desde el punto de vista de la seguridad para cumplir con las necesidades del negocio de cada empresa en particular, para poder garantizar que la seguridad sea una parte integral de los sistemas.

- Procesamiento correcto en aplicaciones: En este grupo se presentan cuatro controles, cuya misión es el correcto tratamiento de la información en las aplicaciones de la empresa. Para ello las medidas a adoptar son, validación en la entrada de datos, la implementación de controles internos en el procesamiento de al información para verificar o detectar cualquier corrupción de la información a través de los procesos, tanto por error como intencionalmente, la adopción de medidas par asegurar y proteger los mensajes de integridad de las aplicaciones. Y por último la validación en la salida de datos, para asegurar que los datos procesados, y su posterior tratamiento o almacenamiento, sea apropiado a los requerimientos de esa aplicación.
- Controles criptográficos: Nuevamente se recalca este objetivo de la criptografía de proteger la integridad , confidencialidad y autenticidad de la información. En este caso, a través de dos controles, lo que propone es desarrollar una adecuada política de empleo de estos controles criptográficos y administrar las calves que se emplean de forma consciente.

  El tema de claves criptográficas, como se ha podido apreciar hasta ahora, es un denominador común de toda actividad de seguridad, por lo tanto más aún cuando lo que se pretende es implementar un completo SGSI, por lo tanto es conveniente y muy recomendable dedicarle la atención que evidentemente merece, para lo cual una muy buena medida es desarrollar un documento que cubra todos los temas sobre los cuales los procesos criptográficos participarán de alguna forma y desde el mismo referenciar a todos los controles de la norma en los cuales se hace uso de claves. Este documento "rector" de la actividad criptográfica, evitará constantes redundancias y sobre todo inconsistencias en la aplicación de claves.
- Seguridad en los sistemas de archivos: La Seguridad en los sistemas de archivos, independientemente que existan sistemas operativos más robustos que otros en sus técnicas de archivos y directorios, es una de las actividades sobre las que se debe hacer un esfuerzo técnico adicional, pues en general existen muchas herramientas para robustecerlos, pero no suelen usarse. Es cierto que los sistemas de archivos no son un tema muy estático, pues una vez que un sistema entra en producción suelen hacerse muchas modificaciones sobre los mismos, por esto último principalmente es que una actividad que denota seriedad profesional, es la identificación de **¿Cuáles son los directorios o archivos que no deben cambiar y cuáles sí?**. Esta tarea la he visto en muy, pero muy pocas organizaciones, y puedo asegurar que es una de las que mayores satisfacciones proporciona en el momento de "despertar sospechas" y restaurar sistemas. Suele ser el mejor indicador de una actividad anómala, si se ha planteado bien el interrogante anteriormente propuesto. Si se logra identificar estos niveles de "estaticidad y cambio" y se colocan los controles y auditorías periódicas y adecuadas sobre los mismos, este será una de las alarmas de la que más haremos uso a futuro en cualquier etapa de un incidente de seguridad, y por supuesto será la mejor herramienta para restaurar un sistema a su situación inicial.

  Este grupo de tres controles, en definitiva lo que propone es justamente esto, control de software operacional, test de esos datos y controlar el acceso al código fuente.

- Seguridad en el desarrollo y soporte a procesos: Este apartado cubre cinco controles cuya finalidad está orientada hacia los cambios que sufre todo sistema. Los aspectos calve de este grupo son:
    - Desarrollar un procedimiento de control de cambios.
    - Realización de revisiones técnicas a las aplicaciones luego de realizar cualquier cambio, teniendo especial atención a las aplicaciones críticas.
    - Documentar claramente las restricciones que se deben considerar en los cambios de paquetes de software.
    - Implementación de medidas tendientes a evitar fugas de información.
    - Supervisión y monitorización de desarrollos de software externalizado.
- Administración técnica de vulnerabilidades: Toda vulnerabilidad que sucede en un sistema de información, tarde o temprano se describe con todo lujo de detalles en Internet. Las palabras claves de esto son "tarde o temprano", pues cuanto antes se tenga conocimiento de una debilidad y las medidas adecuadas para solucionarlas, mejor será para la organización.

  Este grupo que solo trata un solo control, lo que propone es adoptar medidas para estar al tanto de estos temas más "temprano" que "tarde". Esta actividad, en la actualidad no requiere esfuerzos económicos si se pone interés en la misma, pero sí requiere mucho tiempo para poder consultar Webs especializadas o leer los mails que llegan si se está subscripto a grupos de noticias de seguridad, o buscar en Internet en foros, etc. Lo importante es que existe un amplio abanico de posibilidades para realizar esta tarea, que va desde hacerlo individualmente hasta externalizarla, y a su vez desde hacerlo "Muy temprano" hasta "demasiado tarde" y en todo este abanico se pueden elegir un sinnúmero de opciones intermedias.

  La norma simplemente nos aconseja plantearse formalmente el tema, análisis la relación coste/beneficio en la empresa para esta tarea y adoptar una decisión coherente dentro del abanico expuesto.

A.13 Administración de los incidentes de seguridad

Todo lo relativo a incidentes de seguridad queda resumido a dos formas de proceder:

- Proteger y proceder.
- Seguir y perseguir.

Este viejo planteo (que hemos mencionado varias veces), viene desde la RFC (Request For Comments) 1244, que fue uno de los primeros estándares que regularizó la Política de Seguridad. Tal vez no sea la mejor traducción de estos dos procederes, pero lo que trata de poner de manifiesto es que ante un incidente, quien no posea la capacidad suficiente solo puede "Proceder y proteger", es decir cerrar, apagar, desconectar, etc…con ello momentáneamente solucionará el problema, pero al volver sus sistemas al régimen de trabajo normal el problema tarde o temprano volverá pues no se erradicaron sus causas. La segunda opción, en cambio, propone verdaderamente "Convivir con el enemigo", y permite ir analizando paso a paso su accionar, llegar a comprender todo el detalle de su tarea y entonces sí erradicarlo definitivamente. Por supuesto este último trabajo, requiere estar preparado y contar con los medios y recursos suficientes.

En definitiva, es esto lo que trata de dejar claro este punto de la norma a través de los cinco controles que agrupa, y subdivide en:

- Reportes de eventos de seguridad de la información y debilidades.

  Como su nombre lo indica, este apartado define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas. Estas metodologías deben ser ágiles, por lo tanto se presupone el empleo de herramientas automatizadas que lo hagan. En estos momentos se poseen muchas de ellas.

  En concreto para que estos controles puedan funcionar de manera eficiente, lo mejor es implantar herramientas de detección de vulnerabilidades, ajustarlas a la organización, para saber con total certeza dónde se es débil y donde no, y a través de estas desarrollar un mecanismo simple de difusión de las mismas a los responsables de su administración y solución, los cuales deberán solucionarlas o justificar las causas para no hacerlo, ante lo cual, esta debilidad pasará a ser tratada por el segundo grupo de este control, es decir una metodología de detección de intrusiones, que será la responsable de generar la alerta temprana, cuando una de esas debilidades sea explotada por personal no autorizado. Estas alertas necesitan también un muy buen mecanismo de gestión, para provocar la respuesta inmediata.

- Administración de incidentes de seguridad de la información y mejoras.

  Si se poseen los dos mecanismos mencionados en el punto anterior, la siguiente tarea es disponer de una metodología de administración de incidentes, lo cual no es nada más que un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas. Todo esto no es eficaz si no se realiza la preparación adecuada, por lo tanto es necesario difundirlo, practicarlo y SIMULARLO, es decir generar incidentes que no hagan peligrar los elementos en producción, tanto sobre maquetas como en planta y poner a prueba todos los eslabones de la metodología. Seguramente aparecerán fallos, zonas grises o brechas de seguridad metodológicas, las cuales la mejor manera de solucionarlas es en "situaciones de paz" y no durante un conflicto real……como se pueda apreciar he escrito en terminología muy militar, pues esto no es ni más ni menos que lo que hacen (o deberían hacer….) durante todo el tiempo de paz las fuerzas armadas, "prepararse para incidencias", pues esta actividad no puede ser improvisada cuando llega la misma sino no hace falta ser militar para deducir que será catastrófico. La preparación militar, en los casos defensivos hace principalmente esto, es decir analizar las posibles metodologías que puede aplicar un enemigo y practicar su contramedida, esto es el entrenamiento militar y a su vez son los denominados "ejercicios militares" en el terreno o en mesas de arena (Léase planta y/o maqueta), que no son otra cosa que simulaciones sobre qué sucedería si reacciono des esta forma u otra. La doctrina militar es milenaria, tiene millones de situaciones vividas, practicadas y estandarizadas, por así llamarlas, por los tantos en los casos en que su analogía con la informática es evidente, no se debe re inventar la rueda, sino aprovechar lo que ya existe, y la preparación ante incidencias es uno de los casos más evidentes de esto. Existe un

muy antiguo refrán que dice "Si quieres vivir en paz, prepárate para la guerra". Es decir, si quieres evitar problemas de seguridad, prepárate para ellos.

A.14 Administración de la continuidad de negocio

Este grupo cubre nuevamente cinco controles y los presenta a través de un solo grupo:

- Aspectos de seguridad de la información en la continuidad del negocio.

  Este grupo tiene como objetivo contemplar todas las medidas tendientes a que los sistemas no hagan sufrir interrupciones sobre la actividad que realiza la empresa. Hoy en día los sistemas informáticos son uno de los pilares fundamentales de toda empresa, independientemente de la actividad que realice, ya se puede afirmar que no existe ninguna que no tenga un cierto grado de dependencia con estas tecnologías. Cualquier anomalía de sus sistemas repercute en el negocio de la empresa y por supuesto esto debería ser lo mínimo posible.

  Lo primero que considera este grupo es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio, esto que tal vez parezca muy intangible o impreciso, no es nada más que considerar los puntos o hitos en los cuales debe incluirse "controles" de seguridad dentro de los procesos de la empresa. Es decir, si una empresa conoce bien su actividad, debe ser capaz de redactar su metodología de trabajo a través de flujos o procesos (Simples diagramas de flujo). En cada una de las líneas que unen este grafo, se debe considerar la seguridad, y verificar si esta influye o no en esta secuencia, si influye es un hito de seguridad y debe ser considerado, evaluado e implementado el control correspondiente. Este punto que se presentó unos renglones arriba como intangible, **puedo asegurar que debe ser el más importante de esta norma**, y es el que desencadenará absolutamente todos los controles de seguridad de la empresa, pues si un control no está relacionado con los procesos de la empresa, no tiene mayor sentido y, peor aún, si no se conocen con exactitud los procesos de la empresa, es muy difícil asegurar los sistemas de la misma.

  Una vez detectada y analizada la inclusión de hitos o controles de seguridad en los procesos de la empresa, el segundo paso es evaluar los riesgos que impone este para la interrupción del negocio de la organización, de ese riesgo se derivará un impacto, cuyas consecuencias se deberá determinar cómo asumir.

  Las medidas o determinaciones que se adopten para solucionar, minimizar, mejorar o asumir esos riesgos deberán expresarse por medio de planes de continuidad de negocio (o planes de contingencia), los cuales tienen el objetivo de mantener y restaurar el nivel operacional de la empresa, por medio de un conjunto de medidas que reflejen la forma de proceder y/o escalar ante la ocurrencia de cualquiera de los efectos que produciría un fallo en esos hitos.

  Por último, al igual que el grupo anterior, todas estas medidas, deberán ser puestas a prueba para mantener "vivo" y mejorar este plan.

A.15 Marco Legal y buenas prácticas (legales, de estándares, técnicas y auditorías)

Este grupo cubre diez controles. Es uno de los aspectos más débiles que en estos momentos posee la norma, pues la aplicación de la misma en cada País, debe estar de acuerdo a las bases y regulaciones legales del mismo, las cuales sólo son consideradas, una vez que las organizaciones de estandarización correspondientes adecuan el estándar Inglés a cada País respectivo. Para poner como ejemplo, en el caso de España, no puede (o no debería) ser posible la certificación de una empresa que no de cumplimiento a la LSSI, LOPD, leyes de regulación de las telecomunicaciones, interceptación legal, etc…Estos aspectos ningún auditor certificado en BSI, ISACA internacionalmente, etc. tiene porqué conocerlos, como tampoco tendrá la base suficiente para controlarlos con la rigurosidad que esto implica, y por lo tanto, puede suceder (¿o ya sucede?....) que existan empresas que se estén certificando en esta norma y no cumplan estrictamente con las bases legales de cada País. ¿Qué sucedería si les cae una auditoría de, por ejemplo, la Agencia Protectora de Datos y resulta que no están bien en este aspecto?, ¿Seguiría siendo válida su certificación??? (huuuuummmmm…..)

Llamado a la solidaridad: Por favor AENOR ¡¡¡Apúrese!!!,
(queremos un estándar que se sienta más nuestro).

Hechas las salvedades respectivas, seguimos adelante con este grupo que se encuentra subdividido en:

- Cumplimiento de requerimientos legales.

  Lo primero a considerar aquí es la identificación de la legislación aplicable a la empresa, definiendo explícitamente y documentando todo lo que guarde relación con estos aspectos. Otro componente de este primer grupo es lo relacionado con los derechos de propiedad intelectual (A ver si SGAE se enoja, cosa que puede ser de gravísimas consecuencias…), debiendo generar procedimientos que aseguren el cumplimiento de las regulaciones, el punto tal vez más destacable aquí es el referido al empleo de software legal, su concienciación y difusión.

  Todos los registros que guarden algún tipo de información clasificada desde el punto de vista legal, deben ser protegidos para evitar pérdidas, alteraciones y un aspecto muy importante: "divulgación inadecuada", en particular, y esto ya es una regulación generalizada en todos los Países, los registros de carácter personal y de ello lo más importante es lo que se puede considerar como datos íntimos en el caso de tener necesidad de almacenarlos, como pueden ser enfermedades, discapacidades, orientación religiosa, sexual, política, etc.

  Para todos estos registros, se deben implementar todos los procedimientos necesarios, para prevenir su procesamiento incorrecto, pues se pueden haber considerado todos los aspectos legales en su guarda y custodia, pero al momento de ser procesados, quedan expuestos (memorias temporales, permanencia exterior, o transmisión insegura, etc.), o sus resultados, quedan fuera del perímetro o las evaluaciones de seguridad que fueron realizadas sobre los registros. Por lo tanto, para todo registro deberá ser identificado, analizado, implementado y

documentado, todos los aspectos legales que le aplican, durante el almacenamiento y también en todo momento en que sea requerido para su procesamiento (incluyendo aquí sus desplazamientos).

El último control de este grupo hace referencia a las regulaciones legales que aplican al uso de controles criptográficos. Hoy en día a mi juicio, la ley aplica a tres aspectos de la criptografía:

- El tema de exportación de claves cuyo máximo exponente fue EEUU (hoy en franca decadencia).
- El tema de requerimientos legales sobre registros almacenados y/o en tránsito (Interceptación legal)
- El empleo de claves por parte de los usuarios y administradores de sistemas. Este aspecto es muy pocas veces considerado en las organizaciones, y he conocido ya varios casos de problemas y pleitos legales, por ejemplo, sobre despidos en los cuales una deficiente política de derechos y obligaciones legales de la empresa hacia sus empleados implicó importantes sumas de dinero para poder retomar el acceso/control a sus infraestructuras, y/o descifrar información que sólo estaban en capacidad de hacerlo ciertos empleados. Esto es un aspecto legal que debe ser claramente definido y puesto en conocimiento del personal.

- Cumplimiento de políticas de seguridad, estándares y técnicas de buenas prácticas.

En este grupo a través de dos controles, la norma trata de hacer hincapié en el control del cumplimiento de estas medidas, pues de nada sirve tener todo en regla con los aspectos legales, si luego el personal involucrado no da cumplimiento a las medidas y en definitiva, la implementación falla. Para evitar estas debilidades y los graves problemas que pueden ocasionar, es que se debe asegurar que todos estos procedimientos se cumplan y verificar periódicamente que las regulaciones estén vigentes, sean aplicables y estén de acuerdo con toda la organización.

- Consideraciones sobre auditorías de sistemas de información.

Las auditorías de los sistemas de información son imprescindibles, las dos grandes consideraciones son realizarla de forma externa o interna. Cuando se contrata este servicio a través de empresas externas, los resultados son mejores, pues son su especialidad y por lo tanto tienen en "Know How" necesario y suficiente para detectar los aciertos y errores, la parte negativa es que por los recursos económicos que implica, no pueden ser todo lo periódicas que se desean. Por otro lado, las auditorías internas, no poseen tal vez tanta "expertiz", pero por realizarse con recursos propios, ofrecen la posibilidad de realizarlas con mayor periodicidad e inclusive realizarlas aleatoriamente lo cual suele ser muy efectivo. El aspecto fundamental de una auditoría interna es que no puede estar involucrado el personal responsable de lo que se audita, es decir, no se puede ser "Juez y parte", remarco esto pues, por evidente que parezca no suele cumplirse muy a menudo.

El último tema que considera el estándar es lo referido al empleo de herramientas de auditoría de seguridad. Este es un tema de vital interés desde varios aspectos:

- Una herramienta de auditoría de seguridad instalada, puede servir para el lado bueno o el "oscuro" de la organización. Por lo tanto, las mismas deberán ser tratadas con todas las precauciones (Inventariadas, identificadas, controladas en su acceso, monitorizadas, desinstaladas, etc.). Pues si un usuario no autorizado, accede a ellas, se le está sirviendo la red en bandeja de plata.
- El empleo de una herramienta de auditoría de seguridad debe ser perfectamente regulado, en cuanto a su alcance, profundidad, potencialidad, horario, fechas, ventanas de tiempo de operación, objetivo, resultados deseados, etc. Pues al igual que en el punto anterior, no puede dejarse librado al azar su uso correcto, caso contrario se puede disparar todo un procedimiento de incidencias, o caerse una infraestructura, etc.
- Se debe coordinar con cada sistema a auditar qué es exactamente lo que se va a hacer sobre este y cuales son los derechos y obligaciones que se poseen en el uso de esa herramienta sobre cada sistema en particular, pues no tiene porqué ser el mismo para todos.
- Se debe regular CONTRACTUALMENTE, en los casos de auditorías externas cuáles son los derechos, obligaciones y responsabilidades en el empleo de las mismas, incluyendo claramente las indemnizaciones por daños y perjuicios que pueden ocasionar en su empleo incorrecto.

III. RESUMEN y CONCLUSIONES FINALES.

- Se reitera una vez más, que como se pudo apreciar a lo largo de todos los artículos, 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.

- Algo que no se puede dejar de mencionar de esta norma, es que a través de esta nueva organización de controles, con el objetivo de llevar adelante un verdadero SGSI, es (por primera vez a mi juicio) aplicable a cualquier tipo de organización, independientemente de su magnitud, pues si es grande, tiene todo el nivel de detalle que desea y si es pequeña tiene a su disposición la posibilidad de justificar todo aquello que no le aplica y (una vez planteado y pensado), dejarlo de lado si no le es útil.

- Al finalizar todo el análisis e implementación de la norma, el momento crucial es **¿y ahora qué hago?**…….pues se muy simple……..empezar de nuevo (¡esto no es para vagos!), es al fin y al cabo, UN SISTEMA DE GESTIÓN, y todo sistema de gestión es un bucle sin fin, sino no habría nada que gestionar.

- Con toda sinceridad creo que a todo responsable de seguridad, le ha llegado la hora de dejar un poco de lado su perfil técnico y hacerse un hueco para las actividades de gestión de la seguridad. Este estándar es el mejor punto de partida y el que mayores satisfacciones le dará al respecto

- Quedan aún ciertos interrogantes que tal vez, puedan ser mejorados. En estos momentos se está trabajando en nuevos controles, de los que se comentan que serán más de dos cientos (respecto a los ciento treinta y tres actuales), pero todo esto es mejor dejarlo para otro artículo…..

- Por último cierro esta serie de artículos de ISO 27001, con las mismas palabras que los inicié:

> **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**, lo cual es lógico, pues si se desea interrelacionar sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones, se deben exigir mutuamente niveles concretos y adecuados de seguridad informática, sino se abren brechas de seguridad entre sí.....este estándar apunta a poder exigir dichos niveles; y ya no puede caber duda que las empresas, para competir con sus productos (sean de la índole que fueren) en este mercado cibernético actual, tienen cada vez más necesidad de interrelacionar sus infraestructuras de información.....**ISO-27001 en este sentido es una muy buena y sólida opción.**

Alejandro Corletti Estrada - Madrid, **"Navidad"** de 2006.