



Consejos de implantación y métricas de ISO/IEC 27001 y 27002

Realizado por la comunidad internacional de implantadores de ISO27000 de ISO27001security.com

Traducido del original inglés al español por www.iso27000.es

Versión 1, 28 de Junio de 2007

Introducción

Esto es un documento colaborativo creado por implantadores de ISO/IEC 27001 y 27002 pertenecientes al [ISO27k implementers' forum](http://ISO27kimplementersforum.com). Queríamos documentar y compartir algunas recomendaciones pragmáticas para implantar los estándares de gestión de seguridad de la información, además de potenciales métricas para medir y reportar el estado de la seguridad de la información, referenciadas en ambos casos a los estándares ISO/IEC.

Alcance

Esta guía cubre todos los 39 objetivos de control listados en las secciones 5 a 15 de ISO/IEC 27002, además de la sección 4 de evaluación y tratamiento de riesgos que les precede.

Objetivo

Este documento pretende ayudar a otros que estén implantando o planeando implantar los estándares ISO/IEC de gestión de seguridad de la información. Al igual que los propios estándares ISO/IEC, se trata de un documento genérico y necesita ser adaptado a las necesidades específicas de cada uno.

Copyright



Este trabajo tiene copyright © 2007, [ISO27k implementers' forum](http://ISO27kimplementersforum.com), algunos derechos reservados. Está licenciado bajo licencia [Creative Commons Attribution-NonCommercial-Share Alike 3.0](http://creativecommons.org/licenses/by-nc-sa/3.0/). Vd. puede reproducir, distribuir, usar y crear trabajos derivados de este, siempre y cuando (a) no sean vendidos o incorporados en ningún producto comercial, (b) sean correctamente atribuidos al *ISO27k implementers' forum* (www.ISO27001security.com), y (c) sean compartidos bajo los mismos términos que este.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
4. Evaluación y tratamiento de riesgos			
4.1	Evaluación de riesgos de seguridad	Se puede usar cualquier método de gestión de riesgos de seguridad de la información, con preferencia por métodos documentados, estructurados y generalmente aceptados como OCTAVE , MEHARI , ISO TR 13335 ó BS 7799 Parte 3 (y, en su momento, ISO/IEC 27005).	Porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".
4.2	Tratamiento de riesgos de seguridad	La gerencia (específicamente, los propietarios de activos de información) necesita evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones deben documentarse en un Plan de Tratamiento de Riesgos (PTR). Es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información que se estiman dentro de la "tolerancia al riesgo" de la organización, sin que sea éste el enfoque por defecto.	Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia. Costes de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI. Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios.
5. Política de seguridad			
5.1	Política de seguridad de la información	Piense en términos de un manual o <i>wiki</i> de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o auto-evaluación).

Ref.	Objetivo	Consejos de implementación	Posibles métricas
6. Aspectos organizativos de la seguridad de la información			
6.1	Organización interna	Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y <i>Compliance</i> .	<p>Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección.</p> <p>Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.</p>
6.2	Terceros	<p>Haga inventario de conexiones de red y flujos de información significativos con 3^{as} partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos. ¡Esto puede dar miedo, pero es 100% necesario!</p> <p>Considere exigir certificados en ISO/IEC 27001 a los <i>partners</i> más críticos, tales como <i>outsourcing</i> de TI, proveedores de servicios de seguridad TI, etc.</p>	<p>Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.</p>
7. Gestión de activos			
7.1	Responsabilidad sobre los activos	<p>Elabore y mantenga un inventario de activos de información (similar al preparado en su día para el <i>Efecto 2000</i>), mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. ej., ubicación, n^o de serie, n^o de versión, estado de desarrollo / pruebas / producción, etc.).</p> <p>Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.</p>	<p>Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado).</p> <p>Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables.</p>
7.2	Clasificación de la información	<p>¡Mantenga la sencillez! Distinga los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo.</p> <p>Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad.</p>	<p>Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
8. Seguridad ligada a los recursos humanos			
8.1	Antes de la contratación	<p>Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.</p>	<p>Porcentaje de nuevos empleados o <i>pseudo-empleados</i> (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.</p>
8.2	Durante la contratación	<p>La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc.</p> <p>Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.</p>	<p>Respuesta a las actividades de concienciación en seguridad medidas por, p. ej., el número de e-mails y llamadas relativas a iniciativas de concienciación individuales.</p>
8.3	Cese o cambio de puesto de trabajo	<p>Véase Sección 7.1. La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente.</p> <p>Examine qué accesos necesita revocar en primer lugar cuando un empleado presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables?</p> <p>Haga un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).</p>	<p>Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
9. Seguridad física y ambiental			
9.1	Áreas seguras	<p>El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI).</p> <p>Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4ª planta, reténgalo).</p> <p>Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.</p>	<p>Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.</p>
9.2	Seguridad de los equipos	<p>Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita. Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc. Tome en consideración el uso de códigos de barras para hacer los chequeos más eficientes.</p>	<p>Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
10. Gestión de comunicaciones y operaciones			
10.1	Responsabilidades y procedimientos de operación	Documento procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización.	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-).
10.2	Gestión de la provisión de servicios por terceros	¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema de supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio. Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. En algunos casos puede funcionar un sistema de premio y castigo. Esté atento a cambios que tengan impacto en la seguridad.	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.
10.3	Planificación y aceptación del sistema	Adopte procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, etc., usando estándares aceptados como ISO 20000 (ITIL) donde sea posible. Defina e imponga estándares de seguridad básica (mínimos aceptables) para todas las plataformas de sistemas operativos, usando las recomendaciones de seguridad de CIS, NIST, NSA y fabricantes de sistemas operativos y, por supuesto, sus propias políticas de seguridad de la información.	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similares y (b) cuya conformidad con dichos estándares ha sido comprobada mediante <i>benchmarking</i> o pruebas.
10.4	Protección contra código malicioso y móvil	Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación). ¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables!	Tendencia en el número de virus, gusanos, troyanos o <i>spam</i> detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
10.5	Copias de seguridad	<p>Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Báse en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.</p> <p>Encripte copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?).</p>	<p>Porcentaje de operaciones de backup exitosas.</p> <p>Porcentaje de recuperaciones de prueba exitosas.</p> <p>Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales.</p> <p>Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.</p>
10.6	Gestión de la seguridad de las redes	<p>Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.</p>	<p>Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.</p>
10.7	Manejo de los soportes	<p>Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes).</p> <p>Encripte todos los datos sensibles o valiosos antes de ser transportados.</p>	<p>Porcentaje de soportes de backup o archivo que están totalmente encriptados.</p>
10.8	Intercambio de información	<p>Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones <i>offline</i> por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.</p>	<p>Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.</p>
10.9	Servicios de comercio electrónico	<p>Trabaje estrechamente con las unidades de negocio para desarrollar un eBusiness seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de eCommerce, desde el principio (también en cualquier cambio/actualización posterior). Insista en el valor añadido de la seguridad en la reducción de riesgos comerciales, legales y operativos asociados al eBusiness. Trabaje los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad.</p>	<p>"Estado de la eSeguridad", es decir, un informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas, cambios planificados, etc.</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
10.10	Supervisión	El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico. Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.	<p>Porcentaje de sistemas cuyos <i>logs</i> de seguridad (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de <i>logs</i> y (c) son monitorizados/revisados/evaluados regularmente.</p> <p>Tendencia en el número de entradas en los <i>logs</i> de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.</p>
11. Control de accesos			
11.1	Requisitos de negocio para el control de accesos	Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.
11.2	Gestión de acceso de usuario	<p>Cree la función diferenciada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la dirección de seguridad de la información.</p> <p>Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible.</p>	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes").
11.3	Responsabilidades del usuario	Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentadas y (b) formalmente aceptadas.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
11.4	Control de acceso a la red	Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).	Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).
11.5	Control de acceso al sistema operativo	Implante estándares de seguridad básica para todas las plataformas informáticas y de comunicaciones, recogiendo las mejores prácticas de CIS , NIST , fabricantes de sistemas, etc.	Estadísticas de vulnerabilidad de sistemas y redes, como nº de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias).
11.6	Control de acceso a la aplicación y a la información	Implante estándares de seguridad básica para todas las aplicaciones y <i>middleware</i> , recogiendo las mejores prácticas y <i>checklists</i> de CIS , NIST , fabricantes de software, etc.	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre").
11.7	Ordenadores portátiles y teletrabajo	<p>Tenga políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, <i>laptops</i>, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware.</p> <p>Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.</p>	"Estado de la seguridad en entorno portátil / teletrabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (<i>laptops</i> , PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, <i>firewalls</i> personales, etc.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
12. Adquisición, desarrollo y mantenimiento de los sistemas de información			
12.1	Requisitos de seguridad de los sistemas de información	<p>Involucra a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan. Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien.</p> <p>Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas. Numerosas referencias ofrecen orientación sobre la implementación, como, p. ej., OWASP.</p>	Ver 11.1
12.2	Procesamiento correcto en las aplicaciones	<p>Siempre que sea posible, utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc.</p> <p>Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control).</p> <p>Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc.</p>	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.
12.3	Controles criptográficos	<p>Utilice estándares formales actuales tales como AES, en lugar de algoritmos de cosecha propia.</p> <p>¡La implementación es crucial!</p>	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses).
12.4	Seguridad de los archivos de sistema	<p>Aplique consistentemente estándares de seguridad básica, asegurando que se sigan las recomendaciones de CIS, NIST, fabricantes de sistemas, etc.</p>	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares.

Ref.	Objetivo	Consejos de implementación	Posibles métricas
12.5	Seguridad en los procesos de desarrollo y soporte	<p>Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.</p> <p>Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).</p>	<p>"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.</p>
12.6	Gestión de la vulnerabilidad técnica	<p>Haga un seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update o Secunia Software Inspector). Evalúe la relevancia y criticidad o urgencia de los parches en su entorno tecnológico. Pruebe y aplique los parches críticos, o tome otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente. Evite quedarse tan atrás en la rutina de actualización de versiones que sus sistemas queden fuera de soporte por el fabricante.</p>	<p>Latencia de parcheo o semiperíodo de despliegue (tiempo que ha llevado parchear la mitad de los sistemas vulnerables -evita variaciones circunstanciales debidas a retrasos en unos pocos sistemas, tales como portátiles fuera de la empresa o almacenados-).</p>
13. Gestión de incidentes en la seguridad de la información			
13.1	Notificación de eventos y puntos débiles de la seguridad de la información	<p>Establezca y dé a conocer una <i>hotline</i> (generalmente, el <i>helpdesk</i> habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad.</p>	<p>Estadísticas del <i>helpdesk</i> de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
13.2	Gestión de incidentes de seguridad de la información y mejoras	Las revisiones post-incidente y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.	<p>Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida.</p> <p>Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.</p>
14. Gestión de la continuidad del negocio			
14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	<p>Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.).</p> <p>Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio.</p> <p>Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de <i>failover</i>, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.</p> <p>Obtenga consejos de implantación en BS 25999 - Gestión de la Continuidad de Negocio.</p>	<p>Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado).</p> <p>Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante tests apropiados en los últimos 12 meses.</p>

Ref.	Objetivo	Consejos de implementación	Posibles métricas
15. Cumplimiento			
15.1	Cumplimiento de los requisitos legales	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.	<p>Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).</p> <p>Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.</p>
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.	<p>Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).</p> <p>Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.</p>
15.3	Consideraciones de las auditorías de los sistemas de información	<p>Invierta en auditoría TI cualificada que utilice ISO 27001, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación.</p> <p>Examine ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental" como fuente valiosa para la realización de auditorías internas del SGSI. ISO 19011 proporciona un marco excelente para crear un programa de auditorías internas y contiene asimismo las cualificaciones del equipo de auditoría interna.</p>	<p>Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).</p> <p>Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo.</p> <p>Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.</p>
*** Fin de la tabla ***			

Referencias de fuentes adicionales de información

Berinato, S. (2005). "A Few Good Metrics". CIO-Asia, Septiembre. Centrado en la selección y medida de unas pocas métricas útiles, antes que un gran número de ellas inútiles. Ideas creativas de presentación en informes a la dirección.

Berinato, S., Campbell, G., Mena, C., y Lefler, D. (2005). "Influencing Senior Management - Security Metrics". Presentación al CSO Executive Council. Consejos en la selección de métricas de seguridad S.M.A.R.T. [específicas -*Specific*-, medibles -*Measurable*-, alcanzables -*Achievable*-, relevantes -*Relevant*- y delimitadas en el tiempo -*Time bound*-] que sean reducidas en número, actuales y precisas, validadas y aprobadas por las partes interesadas y (sobre todo) útiles.

Hinson, G. (2006). "7 Myths About Security Metrics". ISSA Journal, Julio. Plantea consideraciones de diseño de un sistema de métricas de seguridad, con algunos ejemplos.

Hauser, J.R. and Katz, G.M. (1998). "Metrics: You Are What You Measure". MIT. Un artículo para la reflexión que avisa sobre los peligros de conducir un proceso en una dirección no pretendida, por el uso de métricas inapropiadas.

[ISO/IEC 27001:2005](#). "International standard - Information technology - Security techniques - Information security management systems - Requirements".

[ISO/IEC 27002:2005](#). "International standard - Information technology - Security techniques - Code of practice for information security management" [anteriormente conocida como ISO/IEC 17799:2005].

[NIST](#) (National Institute of Standards and Technology) (2003). "Security Metrics Guide for Information Technology Systems". [Special Publication 800-55](#). Incluye una lista extraordinariamente exhaustiva de posibles métricas (pero, desafortunadamente, no ayuda mucho en cómo seleccionar métricas *útiles*). El primer borrador público de la [Special Publication 800-80](#) "Guide for Developing Performance Metrics for Information Security" está disponible para comentarios.

Registro de cambios

Versión 1, 28 de Junio de 2007

Publicado por el [ISO27k implementers' forum](#). Aportaciones de Gary Hinson, H Deura, K, Ramiah Marappan, Rainier Vergara y Richard O. Regalado.

Traducido del original inglés al español por Javier Ruiz Spohr (www.iso27000.es). 16 de Noviembre de 2007.

Feedback

Comentarios, preguntas y sugerencias de mejora (¡especialmente, sugerencias de mejora!) son bienvenidas a través del [ISO27k implementers' forum](#) o, directamente, al administrador del foro Gary@isect.com