Securing Business

I-SEC Information Security Inc.

Normas y Estándares de Seguridad Relacionados con la gestión de Base de Datos

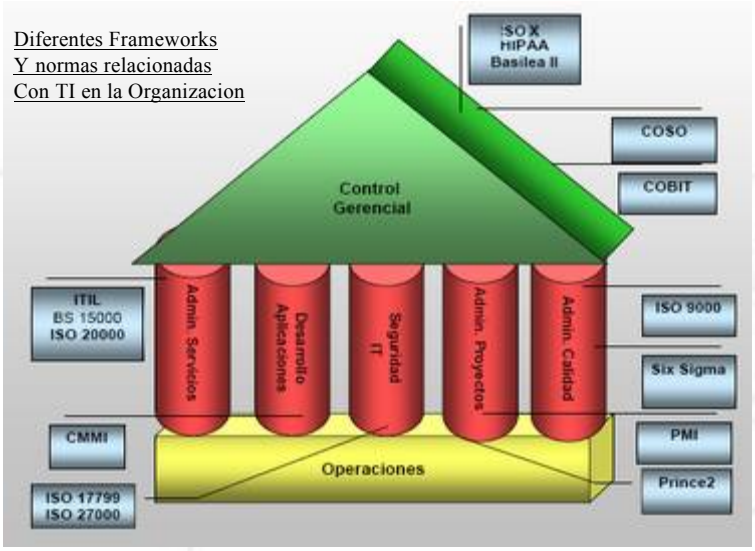
Frano Capeta Mondoñedo, Lead Auditor ISO 27001

I-SEC Information Security
Country Manager & Security Senior Consultant

Securing Business

I-SEC Information Security Inc.

Diferentes Frameworks
Y normas relacionadas
Con TI en la Organizacion



www.isec-global.com
COPYRIGHT 2000-20008 / I-SEC INFORMATION SECURITY S.A

Securing Business

ISO 27001 & ISO 27002

- Gestion de la seguridad de Informacion
  - En Peru se denomina ISO 17799:2007

DOMINIOS NTP/ISO 17799:2007

A5. Política de Seguridad
A6. Organización de Seguridad
A7. Administración de Activos
A8. Seguridad de los Recursos Humanos
A9. Seguridad Física y Ambiental
A10. Gestión de Comunicaciones y Operaciones
A11. Sistema de Control de Accesos
A12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
A13. Administración de Incidentes de Seguridad de la Información
A14. Plan de Continuidad del Negocio
A15.Cumplimiento

I-SEC Information Security Inc.

Securing Business

Controles Específicos :

A.10.10.1 Registro de auditoria

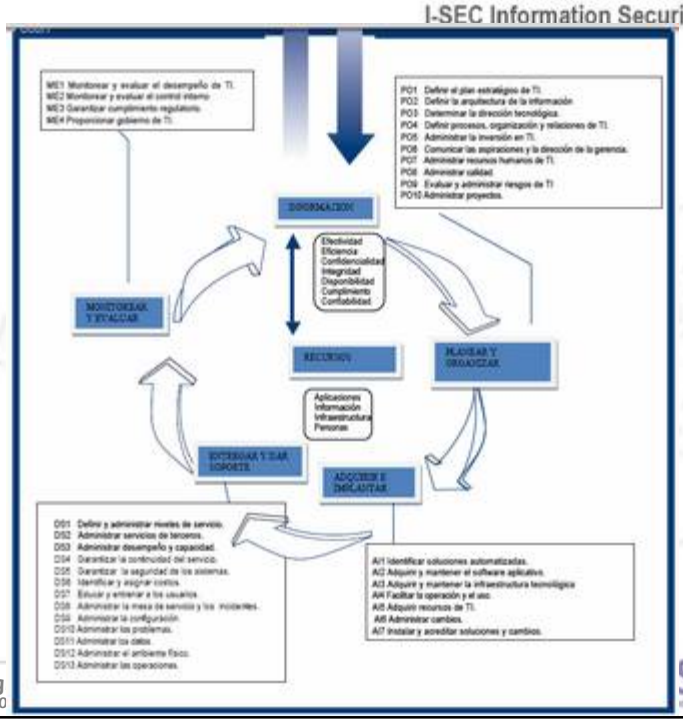
A.12.2.4 Protección de la data de prueba del sistema

www.isec-global.com
COPYRIGHT 2000-20008 / I-SEC INFORMATION SECURITY S.A

Securing Business

COBIT

I-SEC Information Security Inc.



Securing Business

DS5 Entregar y dar soporte
Garantizar la seguridad de los sistemas

Objetivos de control detallados

DS5 Garantizar la seguridad de los sistemas

DS5.1 Administración de la seguridad de TI
Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI
Traducir los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

DS5.3 Administración de identidad
Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos del en este entorno con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son validados por la gerencia del usuario, apropiados por el responsable del sistema e implementados por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementa y se mantiene actualizando medidas técnicas y procedimientos restrictivos, para establecer la identificación del usuario, realizar la autenticación y fortalecer los derechos de acceso.

DS5.4 Administración de cuentas del usuario
Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tratados en cuanto por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa el responsable de los datos o del sistema cómo otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de registro al sistema (registros) y de monitoreo permite la detección oportuna de actividades anormales o esperadas que pueden requerir atención. El acceso a la información de registro al sistema está alineado con los requerimientos del negocio en relación de requerimientos de retención y de derechos de acceso.

DS5.6 Definición de incidente de seguridad
Garantizar que las características de los posibles incidentes de seguridad sean definidos y comunicados de forma clara, de manera que los problemas de seguridad sean tratados de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

DS5.7 Protección de la tecnología de seguridad
Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que almacene un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de llaves criptográficas
Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implementados, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, detección y corrección de software malicioso
Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para protegerse a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado intencionalmente, etc.).

DS5.10 Seguridad de la red
Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos sensitivos
Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

Securing Business

DS11 Entregar y dar soporte
Administración de datos

Objetivos de control detallados

DS11 Administración de la información

DS11.1 Requerimientos del negocio para administración de datos
Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

DS11.2 Acuerdos de almacenamiento y conservación
Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encripción y autenticación.

DS11.3 Sistema de administración de librerías de medios
Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

DS11.4 Eliminación
Definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse.

DS11.5 Respaldo y restauración
Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

DS11.6 Requerimientos de seguridad para la administración de datos
Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

Securing Business

I-SEC Information Security Inc.

PCI Security Standards Council

El estándar PCI fue creado originariamente para proteger la información sensible de las tarjetas de crédito, para reducir el fraude e identificar los problemas de seguridad que podrían ser explotados por usuarios maliciosos.

Cualquier negocio en el que se procese, almacene y transmita información de tarjetas de crédito y transaccional debe cumplir con el estándar PCI con el fin de mantener los derechos y encontrarse autorizado para gestionar el pago mediante tarjeta de crédito.

El standard PCI-DSS define 12 requerimientos básicos separados en 6 categorías. Los mismos abarcan todas las áreas involucradas en la seguridad del procesamiento de transacciones con tarjetas de pago.

Securing Business

I-SEC Information Security Inc.

PCI Data Security Standard (DSS)

Categoría 2: Proteger la Información del Titular de Tarjetas de Pago

3) Proteger Información Almacenada.

- Minimizar el almacenamiento de datos de titulares de tarjetas
- Restricciones de almacenamiento de datos sensibles (Track1 / Track2, CVV2, PIN Block, Account Numbers, etc)
- Enmascarar el "Primary Account Number" (PAN) al mostrarlo (primeros 6 y últimos 4 dígitos)
- Uso de algoritmos de encripción estándar de la industria
- Documentar e implementar procedimientos de manejo de claves.

4) Cifrar datos del titular de tarjetas e información sensitiva al enviarla por redes públicas

- Usar criptografía fuerte y técnicas de encripción
- No enviar información de titulares de tarjeta por mail sin encripción.

Securing Business

I-SEC Information Security Inc.

ITIL / ISO 2000

Estrategia de Servicio

Gestión Financiera de Servicios de TI

Diseño del Servicio

Gestión de Capacidad
Gestión de Disponibilidad
Gestión de continuidad
Gestión de seguridad
Gestión de Niveles de servicio

Operación del Servicio

Service desk
Gestión de Incidentes
Gestión de problemas

Transición del Servicio

Gestión de cambios
Gestión de Versiones
Gestión de Configuración

I-SEC Information Security Inc.

Normas y Estándares de Seguridad Relacionados con la gestión de Base de Datos

Frano Capeta Mondoñedo, Lead Auditor ISO 27001

I-SEC Information Security
Country Manager & Security Senior Consultant

Si desea una copia de esta presentación solicitela al siguiente correo: frano.capeta@i-secperu.com

Securing Business