Controles Técnicos Requeridos por la LOPD y la ISO 27001

Roberto Soriano

Presidente

ISACA Valencia

Fecha: 27 de mayo de 2009

Roberto Soriano

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- ISACA
  - 02 ISACA 135270, 03 CISA 0331364, 08 CISM 0809073, 08 CobiT-F.
  - Presidente de ISACA Valencia 2008-2010
  - Newsletter 2004-2006. CISA 2006-2008
  - Miembro fundador de ISACA, Perteneciente al comité de redacción de estatutos de ISACA-CV.
  - Profesor de 6 ed del CISA, Profesor de 3 Ed de CobiT
- Experiencia Profesional
  - Gerente
  - Trabaja en TI desde 2001.
  - Implantaciones y Auditorias de cumplimiento de LOPD, Implantaciones de CobiT, Auditorias de SI (Hacking Ético, Controles Generales, Código Fuente, ...)
  - Docente en Master, Postgrados y Cursos Especializados. Profesor en ESAT.

Charla

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- La ley LOPD y la norma ISO 27001 requieren de medidas técnicas de seguridad para su cumplimiento. Veremos cuales son las implementaciones más habituales de estas medidas y por qué son necesarias.
  - No se pretende realizar un estudio de todos los casos posibles. Solo se analizaran posibles soluciones en casos generales.
  - Se hará referencia en cada caso a la ISO con algunas de las partes similares del Real Decreto de 2007 de la LOPD.
  - Se analizaran requerimientos y se plantearan posibles soluciones entre todos a modo de ejercicio.

Política de Seguridad

1. Política de Seguridad de la Información (SI).
   - Ref: ISO 27001 P5 y RD1720/2007 LOPD Art 88
   - Objetivo:

     Proporcionar dirección gerencial y apoyo a la seguridad de la información de acuerdo a los requerimientos comerciales y leyes y regulaciones relevantes

   1. Documentar la política de seguridad de la información
      - *Gerencia aprueba documento de política, se publica y comunica a empleados e interesados.*
   2. Revisar la política de seguridad de la información
      - *Se revisa la política de seguridad de la información regularmente en periodos planeados o tras cambios significativos, parea asegurar la continua idoneidad, eficiencia y efectividad.*

Organización de la SI

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Organización Interna
   - Ref: ISO 27001 P6 y RD1720/2007 LOPD Art 89, ...
   - Objetivo:

     Manejar la seguridad de la información dentro de la organización

   1. Compromiso de gerencia
      - *Dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades.*
   2. Coordinación de SI
      - *Por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.*
   3. Asignación de responsabilidades de SI
      - *Definir claramente las responsabilidades de SI*
   4. Proceso de autorización para los medios de procesamiento
      - *Definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información*

Organización de la SI

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Organización Interna
   - Continuación
   5. Acuerdos de confidencialidad
      - *Identificar y revisar regularmente los requerimientos de confidencialidad o no divulgación*
   6. Contacto con autoridades
      - *Mantener los contactos apropiados con las autoridades relevantes*
   7. Contacto con interesados
      - *Mantener los contactos apropiados con los grupos de interés*
   8. Revisión independiente
      - *Revisar de forma independiente a intervalos planeados o cuando sucedan cambios significativos.*

Organización de la SI

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

2. Entidades externas
   - Ref: ISO 27001 P6 y RD1720/2007 LOPD Art 83, ...
   - Objetivo:

     Mantener la SI de la organización y los medios de procesamiento de información a los que entidades externas tienen acceso y procesan; o son comunicados o manejados por entidades externas.

   1. Identificación de riesgos relacionados con entidades externas
      - *Identificar riesgos de la información y sistemas de procesamiento e implementar controles apropiados antes de otorgar acceso*
   2. Tratamiento de la seguridad cuando se trabaja con clientes
      - *Tratar los requerimientos de seguridad identificados antes de otorgar acceso a los clientes*
   3. Tratamiento de la seguridad en contratos con terceras personas
      - *Acuerdos sobre acceso, procesamiento, comunicación o manejo por terceros a la información o a los sistemas. Deben abarcar los requerimientos de seguridad necesarios.*

Gestión de activos

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Responsabilidad por los activos.
   - Ref: ISO 27001 P7 y RD1720/2007 LOPD Capitulo 5
   - Objetivo:

     Lograr y mantener la protección apropiada de los activos.

   1. Inventarios de activos
      - *Identificación de todos los activos. Elaborar y mantener inventario de todos los activos importantes.*
   2. Propiedad de los activos
      - *Asignar la propiedad de la información y activos a parte designada de la organización*
   3. Uso aceptable de los activos
      - *Identificar, documentar e implementar reglas para uso de la información y activos asociados.*

Gestión de activos

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Clasificación de la información.
   - Ref: ISO 27001 P7 y RD1720/2007 LOPD Capítulo 5
   - Objetivo:

     Asegurar que la información reciba un nivel de protección apropiado.

   1. Alineamientos de clasificación
      - *Clasificar la información según su valor, requerimientos legales, confidencialidad y criticidad.*
   2. Etiquetado y manejo de la información
      - *Desarrollar e implementar procedimientos de etiquetado y manejo de la información según el esquema de la organización*

Seguridad de RRHH

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Antes del empleo
   - Ref: ISO 27001 P8 y RD1720/2007 LOPD Art 88, 89, 91, 123, ...
   - Objetivo:

     Asegurar que los trabajadores entiendan sus responsabilidades, sean adecuados para los roles contratados y reducir riesgos.

   1. Roles y responsabilidades
      - *Definir y documentar los roles y responsabilidades de seguridad según la política de seguridad de la organización.*
   2. Selección
      - *Verificar los antecedentes de los candidatos según las leyes, regulaciones y ética relevante. Proporcionales a requerimientos comerciales, clasificación de la información a la que se va a acceder y riesgos percibidos..*
   3. Términos y Condiciones de Empleo
      - *Deben aceptar y firmar los términos y condiciones del contrato. Donde se establecerán las responsabilidades del empleado y la empresa en Seguridad de la información.*

Seguridad de RRHH

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

2. Durante el empleo
   - Ref: ISO 27001 P8 y RD1720/2007 LOPD Art 88, 89, 91, 123, ...
   - Objetivo:

     Asegurar que estén al tanto de amenazas e inquietudes en SI, responsabilidades y obligaciones, y están capacitados para apoyar la política de SI en su trabajo normal y reducir riesgos de error humano.

   1. Gestión de responsabilidades
      - *Gerencia debe requerir que apliquen seguridad según políticas y procedimientos establecidos.*
   2. Capacitación y educación en SI
      - *Recibirán el conocimiento, capacitación y actualizaciones regulares convenientes de políticas y procedimientos según su función laboral.*
   3. Proceso disciplinario
      - *Existirá proceso disciplinario para los que violen la seguridad.*

Seguridad de RRHH

3. Finalización o cambio de empleo
   - Ref: ISO 27001 P8 y RD1720/2007 LOPD Art 88, 89, 91, 123, ...
   - Objetivo:

     Asegurar que la finalización de empleo sea ordenada.
   1. Responsabilidad de Terminación
      - *Definir y asignar las responsabilidades a realizar en la finalización.*
   2. Devolución de activos
      - *Devolverán todos los activos que posean de la organización.*
   3. Eliminación de derechos de acceso
      - *Se eliminaran los derechos de acceso en el momento de finalización.*

Seguridad Física y Ambiental

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Áreas Seguras
   - Ref: ISO 27001 P9 y RD1720/2007 LOPD 91, 92, 99, 107, 108, ...
   - Objetivo:

     Evitar el acceso físico no autorizado, daño e interferencia al local e información .

   1. Perímetro de seguridad física
      - *Uso de paredes, puertas controladas o recepcionistas que protejan áreas con información y medios de procesamiento.*
   2. Controles de entrada físicos
      - *Uso de sistemas que garanticen acceso único a personal autorizado.*
   3. Seguridad de oficinas, habitaciones y medios
      - *Diseñar y aplicar seguridad física.*
   4. Protección contra amenazas externas y ambientales
      - *Protección contra fuego, inundación, terremoto, explosión, disturbios, …*
   5. Trabajo en áreas seguras
      - *Diseño y aplicación de protección física y alineamientos para trabajar en área segura.*
   6. Áreas de acceso publico, entrega y carga
      - *Control de los puntos de acceso, donde personal no autorizado puede ingresar al local, y aislar de los medios de proceso.*

Seguridad Física y Ambiental

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

2. Seguridad del Equipo
   - Ref: ISO 27001 P9 y RD1720/2007 LOPD 91, 92, 99, 107, 108, ...
   - Objetivo:
     Evitar perdida, daño, robo, compromiso de activos e interrupción de actividades.

   1. Ubicación y protección del equipo
      - *Para reducir riesgos de amenazas, peligros ambientales y accesos no autorizados.*
   2. Servicios Públicos
      - *Protegido frente a cortes de energía y otras interrupciones.*
   3. Seguridad en el cableado
      - *Tanto de la energía como datos se deben proteger de interrupción o daño.*
   4. Mantenimiento del equipo
      - *Asegurar continua disponibilidad e integridad*
   5. Seguridad del equipo fuera del local
      - *Aplicar seguridad necesaria que garantice las mismas condiciones internas.*
   6. Eliminación segura o reutilización del equipo
      - *Control de los puntos de acceso, donde personal no autorizado puede ingresar al local, y aislar de los medios de proceso.*
   7. Extraer de la propiedad
      - *Se debe obtener la adecuada autorización previa.*

Gestión de las comunicaciones y operaciones

1. Procedimientos y responsabilidades operacionales
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:

     Asegurar operación correcta y segura de los medios de procesamiento.

   1. Procedimientos de operación documentados
      - *Documentar y mantener los procedimientos. Para quien los necesite.*
   2. Gestión de cambio
      - *Controlar los cambios en los medios y sistemas.*
   3. Segregación de funciones
      - *Reducir riesgo de modificación no autorizada, mal uso, ...*
   4. Separación de los entornos de desarrollo y operacionales
      - *Desarrollo, prueba y operacional. No autorizado o cambios en real.*

Gestión de las comunicaciones y operaciones

2. Gestión de la entrega de servicio de terceros.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:

     Implementar y mantener seguridad según contratos de servicio.

   1. Entrega del servicio
      - *Asegurar que implementan, operan y mantienen según contrato.*
   2. Monitoreo y revisión de los servicios de terceros
      - *Regularmente servicios, informes y registros. Auditoria regular.*
   3. Manejar cambios en los servicios de terceros
      - *Mantenimiento y mejora de políticas, procedimientos, ...*

Gestión de las comunicaciones y operaciones

3. Planeación y aceptación del sistema.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:
     Minimizar el riesgo de fallos en los sistemas.
   1. Gestión de capacidad
      - *Monitorizar y ajustar uso de recursos para asegurar desempeño.*
   2. Aceptación del sistema
      - *Establecer criterios de aceptación para nuevos y actualizaciones y test.*
4. Protección contra software malicioso y código móvil.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:
     Proteger la integridad del software y la información.
   1. Controles contra software malicioso
      - *Detección, prevención y recuperación y procedimientos de concienciación.*
   2. Controles contra códigos móviles
      - *Autorizado y funciona según política.*

Gestión de las comunicaciones y operaciones

5. Respaldo.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:

     Mantener integridad y disponibilidad de los servicios.
   1. Backup
      - *Realizar copias y probar regularmente según política.*
6. Gestión de seguridad de redes.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo:

     Asegurar protección de la información y la infraestructura.
   1. Controles de red
      - *Uso correcto y controlado frente amenazas y seguridad de info.*
   2. Seguridad de los servicios de red
      - *Identificar dispositivos de seguridad, nivel de servicio, requerimiento e indicarlo en contrato.*

Gestión de las comunicaciones y operaciones

7. Gestión de medios.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Evitar divulgación, modificación, eliminación o destrucción no autorizada.
   1. Gestión de medios removibles
      - *Existencia de Procedimiento*
   2. Eliminación de medios
      - *Medios eliminados por procedimiento formal y seguro*
   3. Procedimientos de manejo de la información
      - *Manejo y almacén que proteja la información de divulgación no autorizada*
   4. Seguridad de documentación del sistema
      - *Proteger la documentación de acceso no autorizado*
8. Intercambio de información.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Mantener la SI y software.
   1. Procedimientos y políticas de información y software
      - *Política, procedimientos y controles para proteger el cambio de info.*
   2. Acuerdos de intercambio
      - *Establecer acuerdos para cambio de info y software.*
   3. Medios físicos en transito
      - *Proteger info contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de la organización.*
   4. Mensajes electrónicos
      - *Proteger.*
   5. Sistemas de información comercial
      - *Desarrollar e implantar política y procedimiento para proteger la info en los sistemas comerciales.*

Gestión de las comunicaciones y operaciones

9. Servicios de comercio electrónico.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Asegurar la seguridad de los servicios y uso seguro.
   1. Comercio electrónico
      - *Proteger la info transmitida contra fraude, divulgación, modificación, ...*
   2. Transiciones en línea
      - *Evitar transiciones incompletas, rutas equivocadas, alteración, divulgación, duplicación o reenvío*
   3. Información disponible públicamente
      - *Proteger la integridad de la info para evitar modificación no autorizada*
10. Monitoreo.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Detectar actividades de procesamiento de info no autorizadas.
   1. Registro de auditoria
      - *Proteger la info transmitida contra fraude, divulgación, modificación, ...*
   2. Uso del sistema de monitoreo
      - *Evitar transiciones incompletas, rutas equivocadas, alteración, divulgación, duplicación o reenvío*
   3. Protección de la información del registro
      - *Proteger medios de registro y su información*
   4. Registros del administrador y operador
      - *Registrar actividades del administrador y operador del sistema*
   5. Registros de fallos
      - *Y analizar y llevar acciones correctivas.*
   6. Sincronización de relojes
      - *Equipos relevantes o de dominio de seguridad sincronizados con fuente de tiempo exacta acordada*

Control de acceso

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Requerimiento comercial para el control de acceso.
   - Ref: ISO 27001 P11 y RD1720/2007 LOPD
   - Objetivo: Controlar acceso a la info.
   1. Política de control de acceso

2. Gestión del acceso del usuario.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Autorizar solo a usuarios permitidos y rechazar al resto.
   1. Inscripción del usuario
   2. Gestión de privilegios
   3. Gestión de la clave del usuario
   4. Revisión de los derechos de acceso del usuario

Control de acceso

3. Responsabilidades del usuario.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Evitar acceso no autorizado y compromiso o robo.
   1. Uso de clave
   2. Equipo de usuario desatendido
   3. Política de pantalla y escritorio limpio

4. Control de acceso a redes.
   - Ref: ISO 27001 P10 y RD1720/2007 LOPD
   - Objetivo: Evitar acceso no autorizado a servicios en red.
   1. Política sobre el uso de servicios en red
      - *Solo acceso a servicios autorizados*
   2. Autenticación del usuario para conexiones externas
      - *Métodos de autenticación para controlar acceso de usuarios remotos*
   3. Identificación del equipo en red
      - *Considerar la id automática del equipo para autenticar las conexiones*
   4. Protección del puerto de diagnostico remoto
      - *Control físico y lógico a diagnósticos y configuración*
   5. Segregación de redes
      - *Segregar servicios de info, usuarios y sistemas en la red*
   6. Control de conexión de redes
      - *Restringir conexión de los usuarios*
   7. Control de routing de redes
      - *Asegurar que las conexiones no infringen las políticas de control de acceso*

Control de acceso

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

5. Control de acceso al sistema de operación
   - Registro en terminal, id de usuario, gestión de claves, uso de utilidades de sistema, sesión inactiva, limite de tiempo de conexión
6. Control de acceso a la aplicación e información
   - Restricción de acceso a información, Sistemas sensibles aislados
7. Computación móvil y tele trabajo
   - Políticas de uso de computación móvil y política, plan operacional y procedimientos para tele trabajo

Adquisición, desarrollo y mantenimiento

- Ref: ISO 27001 P10 y RD1720/2007 LOPD Art 21

1. Requerimientos de seguridad de los sistemas
   - Deben especificar requerimientos de controles de seguridad
2. Procesamiento correcto en las aplicaciones
   - Validar datos de entrada, comprobaciones de validación, integridad del mensaje, validar datos de salida
3. Controles criptográficos
   - Política de controles criptográficos, gestión de clave y seguridad de sistema generador
4. Seguridad de los archivos del sistema
   - Control de instalación de software, protección de los datos de prueba, restringir acceso a código fuente.
5. Seguridad en los procesos de desarrollo y soporte
   - Procedimientos de control de cambios, revisión y prueba de las aplicaciones tras cambio de sistema, control de cambios de paquetes soft necesarios y autorizados, evitar filtraciones en la información, supervisar y monitorizar software externo.
6. Gestión de vulnerabilidad técnica
   - Conocer vulnerabilidades, evaluar exposición y tomar medidas apropiadas.

Gestión de incidentes de SI

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Informe de eventos y debilidades
   - Eventos rápidamente a gerencia. Requerir que cualquier empleado reporte debilidad encontrada
2. Gestión de incidentes y mejoras en SI
   - Responsabilidad y procedimiento gerencial que asegure respuesta rápida. Aprender de los incidentes. Recolectar, mantener y presentar evidencias.

Gestión de la continuidad de negocio

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Aspectos de la SI de la gestión de la continuidad de negocio
   - Desarrollar proceso de gestión de continuidad de negocio. Identificar eventos con probabilidad, impacto y consecuencia. En nivel y tiempo requerido tras interrupción. Un solo marco referencial de continuidad. Probar y actualizar.

Cumplimiento

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

1. Cumplimiento con requerimientos legales
   - Identificar legislación aplicable, derechos de propiedad intelectual, proteger registros importantes de la organización, proteger datos y privacidad de información, prevenir mal uso de medios de proceso, uso de controles criptográficos según regulación.
2. Cumplimiento de políticas y estándares de seguridad y cumplimiento técnico
   - Gerentes aseguraran que los procedimientos se realizan correctamente, se comprobara regularmente el cumplimiento con estándares.
3. Consideraciones de auditoria de los sistemas de información
   - Planear los requerimientos y actividades de auditoria y proteger el acceso a las herramientas de auditoria.

ISACA®

Al servicio de los profesionales encargados de la gobernabilidad de la informática

Valencia Chapter

Preguntas

ISACA® 40th ANNIVERSARY
Serving IT Governance Professionals

IT GOVERNANCE INSTITUTE®

COBIT®

CISA®
CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM®
CERTIFIED INFORMATION SECURITY MANAGER®

CGEIT™
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT™