GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter

Controles Técnicos Requeridos por el RDLOPD (RD 1720/2007) y la ISO 27001

Elísabeth Iglesias Domínguez

Consultora / Auditora Técnica

GESDATOS SOFTWARE S.L.

Fecha: 16 de Febrero de 2012

Charla

- El RDLOPD 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.

  – Comenzaremos matizando el “alcance” de las medidas de seguridad obligatorias exigidas en el RDLOPD con los controles exigidos en la ISO 27001

  – Se realizará una comparativa entre las medidas de seguridad exigidas por el RDLOPD y los controles exigidos en la ISO 27001.

  – Veremos una breve comparativa entre la LOPD y la ISO 27001 con el Esquema Nacional de Seguridad (ENS)

ALCANCE RDLOPD VS ISO 27001

- Las medidas de seguridad exigidas en el **RDLOPD** se aplican únicamente a aquellos activos (equipos, soportes, medios electrónicos, instalaciones, personas, etc.) que almacenan, acceden o tratan "**Datos de Carácter Personal**".

- Sin embargo, cuando definimos el **alcance del SGSI** con la **ISO 27001**, vemos como **todos los activos que entran dentro del "Alcance"** definido deben cumplir con los controles y medidas de seguridad exigidos en la norma siempre que así se haya considerado en la Declaración de Aplicabilidad (SOA). El resto de activos que quedan fuera del alcance no tienen porqué someterse, en principio, a las medidas de seguridad que se exigen en dicha norma.

ALCANCE RDLOPD VS ISO 27001

- Por supuesto **la ISO 27001 exige el cumplimiento de la LOPD y de su Reglamento de Desarrollo (**a través de su control A.15.1.4), por lo que, desde este punto de vista, en una implantación de ISO 27001, las medidas de seguridad que exige el RDLOPD serían también exigidas a todos los activos que traten, almacenen, manejen o accedan a datos de carácter personal, aunque sea por ejemplo, un activo de tipo de información (ficheros físicos automatizados o no automatizados) que no se trate en el alcance de la implantación del SGSI.

COMPARATIVA MEDIDAS DE SEGURIDAD RDLOPD VS ISO 27001

Política de Seguridad

1. **Política de Seguridad de la Información (SI).**
   - Ref: ISO 27001 A.5 y RD1720/2007
   - ❖ 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, para asegurar la continua idoneidad, eficiencia y efectividad.*

Documento de Seguridad

1. Documento de Seguridad (DS).

- Ref: RD1720/2007 LOPD Art 88

❖ Objetivo:

1. El responsable del fichero o tratamiento elaborará un **Documento de Seguridad** que recogerá las **medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente** que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento **deberá contener, como mínimo**, los siguientes aspectos:
a. Ámbito de aplicación del documento con especificación detallada de los **recursos protegidos**.
b. **Medidas, normas, procedimientos** de actuación, **reglas y estándares** encaminados a garantizar el nivel de seguridad exigido en este reglamento.

Documento de Seguridad

c. **Funciones y obligaciones del personal** en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d. **Estructura de los ficheros con datos de carácter personal** y **descripción de los sistemas de información que los tratan**.

e. **Procedimiento** de notificación, gestión y respuesta ante las **incidencias**.

f. Los **procedimientos de realización de copias de respaldo** y de recuperación de los datos en los ficheros o tratamientos automatizados.

g. Las **medidas** que sea necesario adoptar **para el transporte de soportes**, así como para la destrucción o la reutilización de los mismos.

Documento de Seguridad

7. El **Documento de Seguridad** deberá mantenerse en todo momento **actualizado y** será **revisado** siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Documento de Seguridad

- En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

  a. La identificación del **responsable o responsables de seguridad**.
  b. Los **controles periódicos** que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento

Organización de la SI

1. Organización Interna

- Ref: ISO 27001 A.6 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

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 grupos de especial interés
      - *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

2. Entidades externas

- Ref: ISO 27001 A.6 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.*

Funciones y Obligaciones del Personal

Funciones y Obligaciones del Personal

- Ref: RD1720/2007 LOPD Art 89
- ❖ Objetivo:

1. Las **funciones y obligaciones** de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
   También **se definirán las funciones de control o autorizaciones** delegadas por el responsable del fichero o tratamiento.

Responsable/s de Seguridad

Responsable/s de Seguridad

- Ref: RD1720/2007 LOPD Art 95
- Objetivo:

1. En el Documento de Seguridad **deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas** en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
   En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Delegación de Autorizaciones

Delegación de Autorizaciones:

- Ref: RD1720/2007 LOPD Art 84
- Objetivo:

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero

Acceso a Datos por cuenta de Terceros

Acceso a datos por cuenta de terceros:

– Ref: RD1720/2007 y LOPD

- Artículo 12 LOPD: Acceso a los datos por cuenta de terceros
- Artículo 20 LOPD: Deber de diligencia del responsable en relación con el encargado
- Artículo 21 LOPD: Subcontratación
- Artículo 22 RDPLOD: Conservación de datos por parte del encargado
- Artículo 83 LOPD: Prestación de servicios sin acceso a datos
- Artículo 88 LOPD: Identificación de encargados en el Documento de Seguridad

Gestión de activos

Responsabilidad por los activos.

- Ref: ISO 27001 A.7 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
   - *Identificar propietarios de la información y de los activos asociados para el tratamiento de la misma.*
3. Uso aceptable de los activos
   - *Identificar, documentar e implementar reglas para uso de la información y activos asociados.*

Gestión de activos

Clasificación de la información.

- Ref: ISO 27001 A.7 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*

Identificación de soportes (etiquetado)

Identificación de Soportes (etiquetado)

- Ref: RD1720/2007 Art 101 (para ficheros de nivel alto)
- Objetivo:

1. La **identificación de los soportes** se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes identificar su contenido, y que dificulten la identificación para el resto de personas

Clasificación de la Información

Clasificación de la Información

- Ref: RD1720/2007 Art 80 y 81 RDLOPD

❖ Objetivo:

- **Artículo 80. Niveles de seguridad.**

  Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

- **Artículo 81. Aplicación de los niveles de seguridad**.

Seguridad de RRHH

1. **Antes del empleo**
   - Ref: ISO 27001 A.8 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. Funciones y responsabilidades
      - *Definir y documentar los roles y responsabilidades de seguridad según la política de seguridad de la organización.*
   2. Investigación de antecedentes de personal
      - *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 Contratación
      - *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

2. Durante el empleo

- Ref: ISO 27001 A.8 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 de Dirección
   - *Gerencia debe requerir que apliquen seguridad según políticas y procedimientos establecidos.*
2. Concienciación, formación y capacitación 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. Cese del empleo o cambio del puesto de trabajo

- Ref: ISO 27001 A.8 y RD1720/2007 LOPD Art 88, 89, 91, 123, ...

❖ Objetivo:

Asegurar que la finalización de empleo sea ordenada.

1. Responsabilidad del cese o cambio
   - *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

1. Áreas Seguras

– Ref: ISO 27001 A.9 y RD1720/2007 LOPD 91, 92, 99, 107, 108, ...

❖ Objetivo:

Evitar el acceso físico no autorizado, daño y las intromisiones en las instalaciones y en la información de la organización

1. Perímetro de seguridad física
   – *Uso de barreras, muros, 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 en las mismas*

Seguridad Física y Ambiental

4. Protección contra amenazas externas y de origen ambiental
   Protección contra fuego, inundación, terremoto, explosión, disturbios, …

5. Trabajo en áreas seguras
   Se deben implantar medidas de protección físicas y las directrices oportunas para trabajar en áreas seguras.

6. Áreas de acceso publico y de carga y descarga
   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

2. Seguridad del Equipo

- Ref: ISO 27001 A.9 y RD1720/2007 LOPD 91, 92, 99, 107, 108, ...

❖ Objetivo:

Evitar perdidas, daños, robos, o circunstancias que pongan en peligro los activos o que puedan provocar interrupción de actividades.

1. Ubicación y protección del equipo
   - *Para reducir riesgos de amenazas, peligros ambientales y accesos no autorizados.*
2. Instalaciones de suministro
   - *Protegido frente a cortes de energía y otras interrupciones.*
3. Seguridad en el cableado
   - *Tanto el cableado eléctrico como el de comunicaciones se deben proteger de interrupción o daño.*
4. Mantenimiento del equipo
   - *Asegurar la continua disponibilidad e integridad (acorde a las especificaciones del proveedor, mantener registro de fallos, etc.)*

Seguridad Física y Ambiental

5. Seguridad del equipo fuera del local

   Aplicar seguridad necesaria que garantice las mismas condiciones internas.

6. Eliminación segura o reutilización del equipo

   Los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado de forma segura antes de su retirada.

7. Retirada de materiales propiedad de la empresa

   Se debe obtener la adecuada autorización previa.

Gestión de las comunicaciones y operaciones

1. **Procedimientos y responsabilidades de operación**
   - Ref: ISO 27001 A.10 y RD1720/2007 LOPD
   - ❖ Objetivo:

     Asegurar operación correcta y segura de los medios de procesamiento.

   Procedimientos de operación documentados
   - *Documentar y mantener los procedimientos de operación, para quien los necesite.*

   1. Gestión de cambios
      - *Controlar los cambios en los medios y sistemas (procedimiento de gestión del cambio).*
   2. Segregación de tareas
      - *Reducir riesgo de modificación no autorizada, usos indebidos, ...*
   3. Separación de los entornos de desarrollo, prueba y operación
      - *El software de desarrollo y de operación debe ejecutarse en distintos sistemas.*
      - *Crear diferentes perfiles de los usuarios en los sistemas operativos y de pruebas.*

Gestión de las comunicaciones y operaciones

2. **Gestión de la entrega de servicio de terceros.**

- Ref: ISO 27001 A.10 y RD1720/2007 LOPD
- Objetivo:

  Implementar y mantener seguridad según contratos de servicio.

1. Provisión de servicios
   - *Asegurar que se implantan los controles oportunos y que los niveles de provisión han sido mantenidos según contrato por parte del tercero.*
2. Monitorización y revisión de los servicios de terceros
   - *Supervisar regularmente servicios, informes y registros. Realizar auditorias periódicas.*
3. Manejar cambios en los servicios de terceros
   - *Mantenimiento y mejora de políticas, procedimientos, reevaluación de riesgos, ...*

Gestión de las comunicaciones y operaciones

3. Planificación y aceptación del sistema.

- Ref: ISO 27001 A.10 y RD1720/2007 LOPD
- ❖ Objetivo:

  Minimizar el riesgo de fallos en los sistemas.

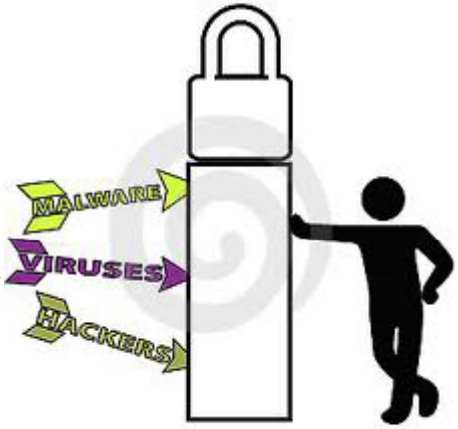
1. Gestión de capacidad
   - *Monitorizar y ajustar uso de recursos para asegurar desempeño.*
2. Aceptación del sistema
   - *Establecer criterios de aceptación para nuevos sistemas y actualizaciones de nuevas versiones y test.*

4. Protección contra software malicioso y código móvil.

- Ref: ISO 27001 A10 y RD1720/2007 LOPD
- ❖ Objetivo:

  Proteger la integridad del software y la información.

1. Controles contra software malicioso
   - *Controles de detección, prevención y recuperación y procedimientos de concienciación.*
2. Controles contra códigos descargados en el cliente
   - *Deben estar autorizados y funcionar según política.*



Gestión de las comunicaciones y operaciones

5. Copias de Seguridad

- Ref: ISO 27001 A.10 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 A10 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 información.*
2. Seguridad de los servicios de red
   - *Identificar dispositivos de seguridad, nivel de servicio, requerimiento e indicarlo en contrato.*
   - *Monitorizar los niveles acordados.*

Gestión de las comunicaciones y operaciones

7. Manipulación de Soportes.

- Ref: ISO 27001 A.10 y RD1720/2007 LOPD
- ❖ Objetivo: Evitar divulgación, modificación, eliminación o destrucción no autorizada de los activos y las interrupciones de las actividades.

1. Gestión de soportes extraíbles
   - *Existencia de Procedimiento*
   - *Etiquetar soportes*
2. Retirada de soportes
   - *Soportes eliminados por procedimiento formal y seguro*
3. Procedimientos de manipulación de la información
   - *Establecer procedimientos para que la manipulación y almacenamiento de la información se realice protegiendo la misma contra la divulgación no autorizada*
4. Seguridad de documentación del sistema
   - *Proteger la documentación del sistema de accesos no autorizados*

Gestión de las comunicaciones y operaciones

8. Intercambio de información.

– Ref: ISO 27001 A.10 y RD1720/2007 LOPD

❖ Objetivo: Mantener la SI y software.

1. Procedimientos y políticas de información y del software
   – *Política, procedimientos y controles para proteger el intercambio de información.*
2. Acuerdos de intercambio
   – *Establecer acuerdos para el intercambio de información y del software entre la organización y terceros*
   – *Definir la propiedad de la información y del software*
3. Soportes físicos en transito
   – *Proteger la información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de las instalaciones de la organización.*
4. Mensajería electrónica
   – *Proteger.*
5. Sistemas de información empresariales
   – *Desarrollar e implantar políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales.*

Gestión de las comunicaciones y operaciones

9. Servicios de Comercio Electrónico.

- Ref: ISO 27001 A.10 y RD1720/2007 LOPD
- ❖ Objetivo: Asegurar la seguridad de los servicios y uso seguro.

1. Comercio electrónico
   - *Proteger la información incluida en el comercio electrónico transmitida a través de redes públicas contra fraude, divulgación, modificación no autorizada, ...*

2. Transiciones en línea
   - *Evitar transiciones incompletas, errores de direccionamiento, alteración, divulgación, duplicación o reenvío (por ejemplo mediante la aplicación de la firma electrónica por cada una de las partes implicadas, cifrado de las comunicaciones, etc.).*

3. Información puesta a disposición pública
   - *Proteger la integridad de la información puesta a disposición pública para evitar modificación no autorizada*

Gestión de las comunicaciones y operaciones

10. Supervisión.

- Ref: ISO 27001 A.10 y RD1720/2007 LOPD
- ❖ Objetivo: Detectar actividades de procesamiento de información no autorizadas.

1. Registro de auditoria
   - *Registros de auditoría de las actividades de los usuarios, las excepciones y eventos*
2. Supervisión del uso del sistema
   - *Supervisar el uso de recursos de procesamiento de la información y revisar periódicamente los resultados de las actividades de supervisión.*
3. Protección de la información del registro
   - *Proteger medios de registro y su información contra manipulaciones,…*
4. Registros del administrador y operador
   - *Registrar actividades del administrador y operador del sistema*
5. Registros de fallos del sistema
   - *Analizar los fallos y tomar acciones correctivas*
6. Sincronización de relojes
   - *Los relojes de todos los sistemas de procesamiento dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada*

Control de Acceso

1. **Requisitos de negocio para el control de acceso.**

   – Ref: ISO 27001 A.11 y RD1720/2007 LOPD
   ❖ Objetivo: Controlar acceso a la información.

   1. Documentar una política de control de acceso

2. **Gestión del acceso del usuario.**

   – Ref: ISO 27001 A.11 y RD1720/2007 LOPD
   ❖ Objetivo: Autorizar solo a usuarios permitidos y rechazar al resto.

   1. Registro del usuario
   2. Gestión de privilegios
   3. Gestión de la clave del usuario
   4. Revisión de los derechos de acceso del usuario a intervalos regulares de tiempo

Control de Acceso

3. Responsabilidades del usuario.

– Ref: ISO 27001 A.11 y RD1720/2007 LOPD

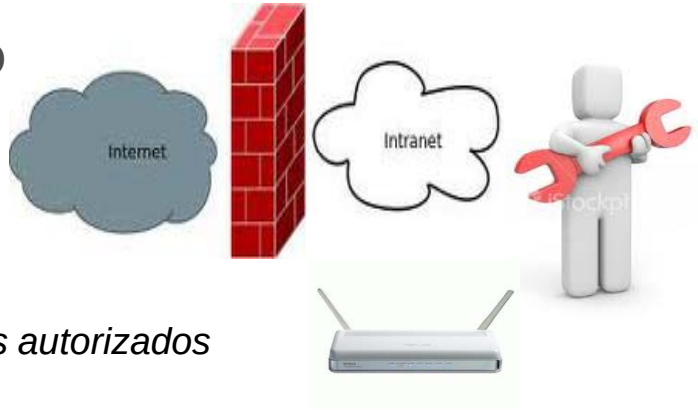
❖ Objetivo: Evitar acceso no autorizado y compromiso o robo.

1. Uso de contraseña
2. Equipo de usuario desatendido
3. Política de puesto de trabajo despejado y escritorio limpio

4. Control de acceso a la red.

– Ref: ISO 27001 A.11 y RD1720/2007 LOPD

❖ Objetivo: Evitar acceso no autorizado a servicios en red.



1. Política sobre el uso de servicios en red

– *Proporcionar acceso a los usuarios solo a servicios autorizados*

Control de Acceso

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. **Diagnóstico remoto y protección de los puertos de configuración**
   Se debe controlar el acceso físico y lógico a los puertos de diagnósticos y configuración

5. **Segregación de redes**
   Segregar servicios de información, usuarios y sistemas en la red

6. **Control de conexión a la red**
   En redes compartidas, restringir la conexión de los usuarios acorde a la política

7. **Control de encaminamiento (routing) de red**
   Asegurar que las conexiones de los ordenadores y los flujos de información no infringen las políticas de control de acceso

Control de Acceso

5. **Control de acceso al sistema operativo**
   - 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 las aplicaciones e información**
   - Restricción de acceso a información, Sistemas sensibles aislados,…
7. **Ordenadores portátiles y teletrabajo**
   - Políticas de uso y procedimientos para computación móvil y teletrabajo

Adquisición, desarrollo y mantenimiento

_ Ref: ISO 27001 A.12 y RD1720/2007 LOPD Art 21

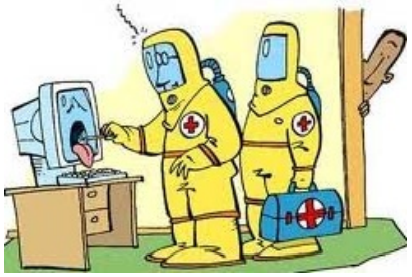
1. **Requisitos de seguridad de los sistemas de información**
   - Deben especificar requisitos de los controles de seguridad
2. **Tratamiento correcto de las aplicaciones**
   - Validar datos de entrada, comprobaciones de validación, integridad del mensaje, validar datos de salida
3. **Controles criptográficos**
   - 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 de los programas.
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 software necesarios y autorizados, evitar filtraciones en la información, supervisar y monitorizar software externo.
6. **Gestión de vulnerabilidad técnica**
   - Conocer vulnerabilidades de los sistemas de información, evaluar la exposición a las mismas y tomar medidas apropiadas.

Gestión de incidentes de Seguridad

-Ref: ISO 27001 A.13

1. **Notificación de eventos y puntos débiles de seguridad de información**
   - Asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.
   - Anotar y notificar cualquier punto débil

2. **Gestión de incidentes y mejoras en SI**
   - Establecer responsabilidades y procedimientos de gestión que asegure respuesta rápida. Aprender de los incidentes. Recopilar, mantener y presentar evidencias.



Gestión de la continuidad de negocio

1. Aspectos de la SI de la gestión de la continuidad de negocio

- **Ref: ISO 27001 A.14**
- Realizar un análisis de impacto (BIA) identificando, cuantificando y priorizando los riesgos.
- 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 para que todos los planes sean coherentes. Probar y actualizar periódicamente.

Cumplimiento

_ Ref: ISO 27001 A.15

1. **Cumplimiento de los requisitos 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 acorde a contratos, leyes y regulaciones.

2. **Cumplimiento de políticas y estándares de seguridad y cumplimiento técnico**
   - Dirección debe asegurarse que los procedimientos se realizan correctamente, se comprobará regularmente el cumplimiento con estándares.

3. **Consideraciones sobre la auditoria de los sistemas de información**
   - Planificar los requisitos y actividades de auditoria en los sistemas y proteger el acceso a las herramientas de auditoria.

RDLOPD VS ISO 27001 VS ENS

❖ RDLOPD

Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

❖ ENS

Sistema de información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

RDLOPD VS ISO 27001 VS ENS

❖ RDLOPD

Lo relevante es el **dato de carácter personal**. Las medidas de seguridad únicamente tienen como objetivo este tipo de información.

❖ ENS

Lo fundamental es el **sistema de información** en su conjunto. Abarca todo tipo de información. El dato de carácter personal es considerado como uno de los tipos de información.

Comparativa ENS - RDLOPD

ENS	RDLOPD
Política de Seguridad Normas de Seguridad Declaración de Aplicabilidad	Documento de Seguridad
Responsable de Seguridad	Responsable de Seguridad
Deberes y obligaciones del personal	Funciones y obligaciones del personal
Identificación única de usuarios	Identificación y autentificación
Autorización y control de accesos	Control de accesos
Auditoría de Seguridad	Auditoría de medidas de seguridad
Gestión de incidencias	Registro de incidencias Procedimiento de notificación, gestión y respuesta ante las incidencias
Protección instalaciones e infraestructura	Control de acceso físico
Protección de los soportes de información	Gestión de soportes y documentos Gestión y distribución de soportes
Protección de aplicaciones informáticas	Pruebas con datos reales
Protección de las telecomunicaciones	Telecomunicaciones

Comparativa ENS – ISO 27001

Marco Organizativo		ISO 27001
Política de Seguridad	org. 1	4.2.1 Creación del SGSI
Normativa de seguridad	org. 2	A.7.1.3 Uso Adecuado de los Activos A.8.2.3 Proceso Disciplinario
Procedimientos de seguridad	org. 3	5.2.2 Concienciación, Formación y Capacitación A. 13 Gestión de Incidentes de Seguridad
Proceso de autorización	org. 4	A.6.1.4 Proceso de Autorización de Recursos para el Tratamiento de la Información A.7.1.3 Uso Adecuado de los Activos A.12 Adquisición, Desarrollo y mantenimiento de los Sistemas de Información A.10.7 Manipulación de Soportes A.11.7 Informática móvil y Teletrabajo

Comparativa ENS – ISO 27001

Marco Operacional		ISO 27001
Planificación	**op.pl**	
Análisis de Riesgos	op.pl. 1	4.2.1 Creación del SGSI
Arquitectura de seguridad	op.pl. 2	A.10.1.1 Documentación de Procedimientos de Operación A.10.7.4 Seguridad de la Documentación A.11 Control de Accesos A.12.2 Tratamiento correcto de Aplicaciones
Adquisición de nuevos componentes	op.pl. 3	A.6.1.4 Proceso de Autorización de Recursos para el Tratamiento de la Información A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información A.10.3 Planificación y Aceptación del Sistema
Dimensionamiento/Gestión de Capacidad	op.pl.4	A.6.1.4 Proceso de Autorización de Recursos para el Tratamiento de la Información A.10.3 Planificación y Aceptación del Sistema
Componentes certificados	op.pl.5	Se establece a nivel de política de adquisición. ETC.

Comparativa ENS – ISO 27001

Medidas de Protección		ISO 27001
Protección de instalaciones e Infraestructuras	**mp.if**	**A.9 Seguridad Física y Ambiental**
Áreas separadas y control de acceso	mp.if. 1	A.9 Seguridad Física y Ambiental
Identificación de personas	mp.if. 2	A.9 Seguridad Física y Ambiental
Acondicionamiento de los locales	mp.if. 3	A.9 Seguridad Física y Ambiental
Energía Eléctrica	mp.if. 4	A.9 Seguridad Física y Ambiental
Protección frente a incendios	mp.if. 5	A.9 Seguridad Física y Ambiental
Protección frente a inundaciones	mp.if. 6	A.9 Seguridad Física y Ambiental ETC.

Roles y Responsabilidades

ENS	RDPLOD	ISO 27001
COMITÉ DE SEGURIDAD, formado por:	•**Responsable de Seguridad**	COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, formado por:
•Responsable de la Información (RINF) •Responsable de Servicios (RSRV) •**Responsable de la Seguridad** (RSEG) •Responsable del Sistema (RSIST)		A.6 Aspectos Organizativos de la Seguridad de la Información A.10 Función diferenciada

Roles y Responsabilidades

“SEGREGACIÓN DE FUNCIONES”

Auditoría RD 1720/2007 vs Auditoría 3/2010

a) **Criterios de categorización diferentes:** tipología de datos (y finalidad en algunas excepciones) vs perjuicio o impacto en sistemas o personas.

a) **Medidas** del RD 1720/2007 son mínimos aplicables SIEMPRE (aunque no se deriven del análisis de riesgos) y las del ENS adicionales si no entran en conflicto.

– 3. ¿Hay que emitir un único informe de auditoría o varios?

Es posible dos o uno en el que se distinga si las deficiencias afectan a una u otra Norma.

Aclaraciones

Otros requisitos recogidos en la Guía de Auditoría CCN-STIC-802:

1. **Si** los sistemas a auditar según el ENS **tratan datos personales se pueden solicitar los informes de auditorías** de protección de datos personales previos.

2. **Si** durante la auditoría del ENS **se detectan no conformidades respecto al RD 1720/2007** debe obligatoriamente comunicarse y constar en el informe de auditoría del ENS (aunque no fuese ése el objetivo inicial).

Conclusiones

- **Podemos hacer coexistir la distinta normativa y sistemas de gestión implantados en la organización teniendo en cuenta:**

  - ✓ Que hay que analizar los puntos comunes y las intersecciones comunes a la diferente normativa.
  - ✓ Concienciación y formación continua de TODOS los usuarios de los sistemas de información en materia de seguridad.
  - ✓ Haciéndonos servir de "*herramientas*" que nos ayuden a la implantación, verificación, mantenimiento, actualización y mejora continua de nuestro sistema de gestión.

de lo contrario……..

"Si no velamos por mantener nuestro sistema de gestión, duro será el trabajo de implantar, pero aún más duro será ver que, con el paso de tiempo, todo el trabajo realizado vaya quedando obsoleto y no haya servido para nada…."

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter

GRACIAS POR SU ATENCIÓN

ISACA®
Serving IT Governance Professionals

IT GOVERNANCE INSTITUTE®

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification