Internet
Red Externa

FTP

Intercambio y Movilidad

Red
Local

Organización

Usuarios

Documentación

Aplicaciones

Puestos de
trabajo

Servidores

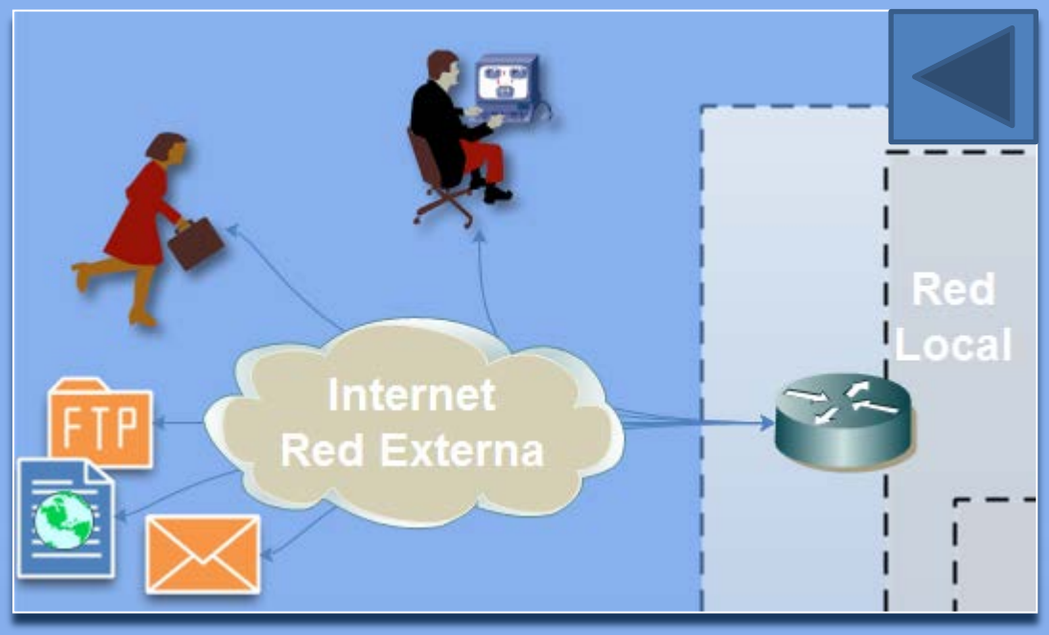
Seguridad Física

Soportes físicos

Servicios externos

Desarrollo y Mantenimiento

www.iso27002.es



Posibles controles relacionados a tener en cuenta:

10.4. Protección contra software malicioso y código móvil

10.6 Gestión de redes

11.4 Control de acceso en red

12.3 Controles criptográficos

Posibles controles relacionados a tener en cuenta :

5.1.1 Documento de política de seguridad de la información

08. Seguridad ligada a los Recursos Humanos

9.2.5 Seguridad de equipos fuera de los locales de la Organización

10.4. Protección contra software malicioso y código móvil

10.8 Intercambio de información y software

11.2 Gestión de acceso de usuario

11.3 Responsabilidades del usuario

11.7 Informática móvil y teletrabajo

12.3 Controles criptográficos

Posibles controles relacionados a tener en cuenta:

9.2.5 Seguridad de equipos fuera de los locales de la Organización
9.2.6 Seguridad en la reutilización o eliminación de equipos
9.2.7 Traslado de activos
10.5 Gestión interna de soportes y recuperación
10.7 Utilización y seguridad de los soportes de información
10.8 Intercambio de información y software
10.9.3 Seguridad en información pública
12.3 Controles criptográficos

Posibles controles relacionados a tener en cuenta:

6.2 Terceros

10.2 Supervisión de los servicios contratados a terceros

10.8.3 Soportes físicos en tránsito

10.8.5 Sistemas de información empresariales

10.9 Servicios de comercio electrónico

99.1 Cloud Computing

Posibles controles relacionados a tener en cuenta:

9.1 Áreas seguras

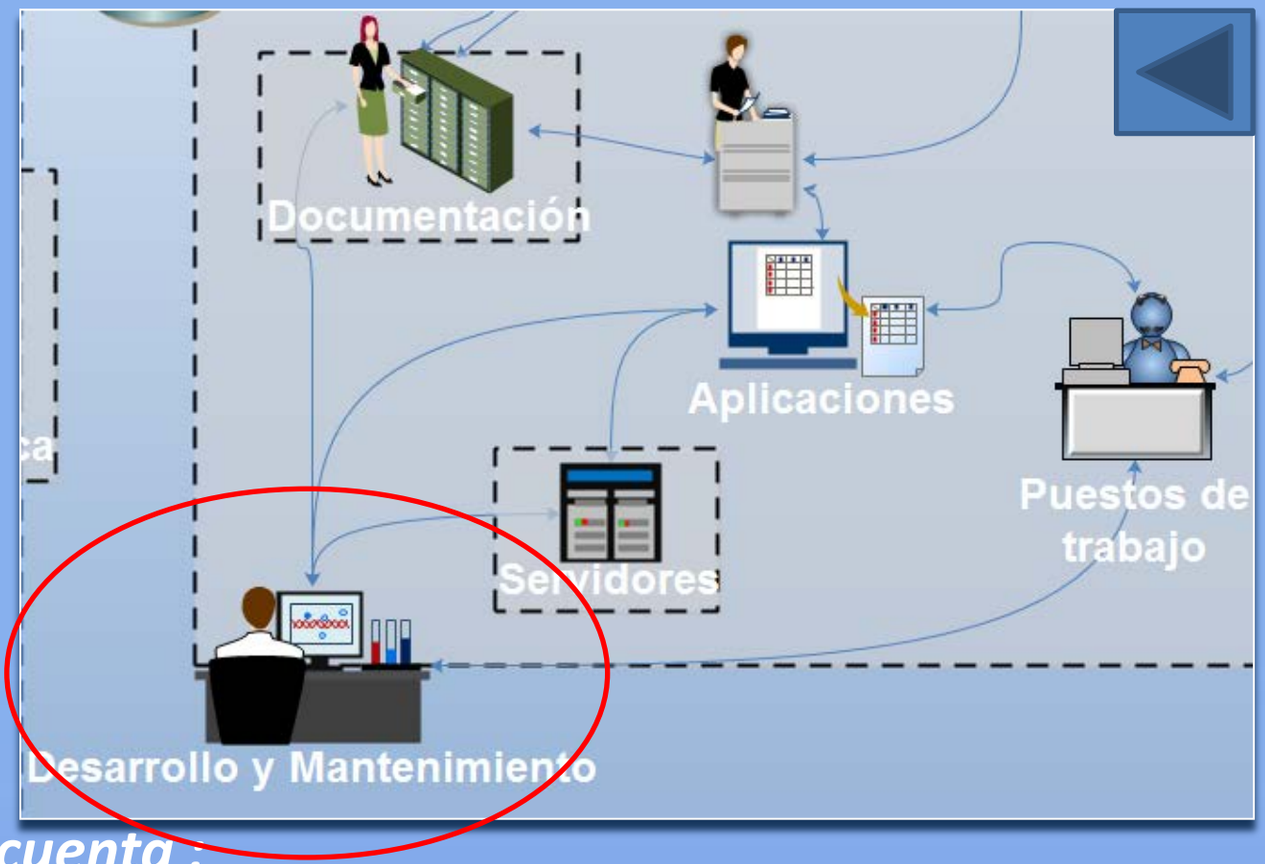
9.2.1 Instalación y protección de equipos

9.2.2 Suministro eléctrico

9.2.3 Seguridad del cableado

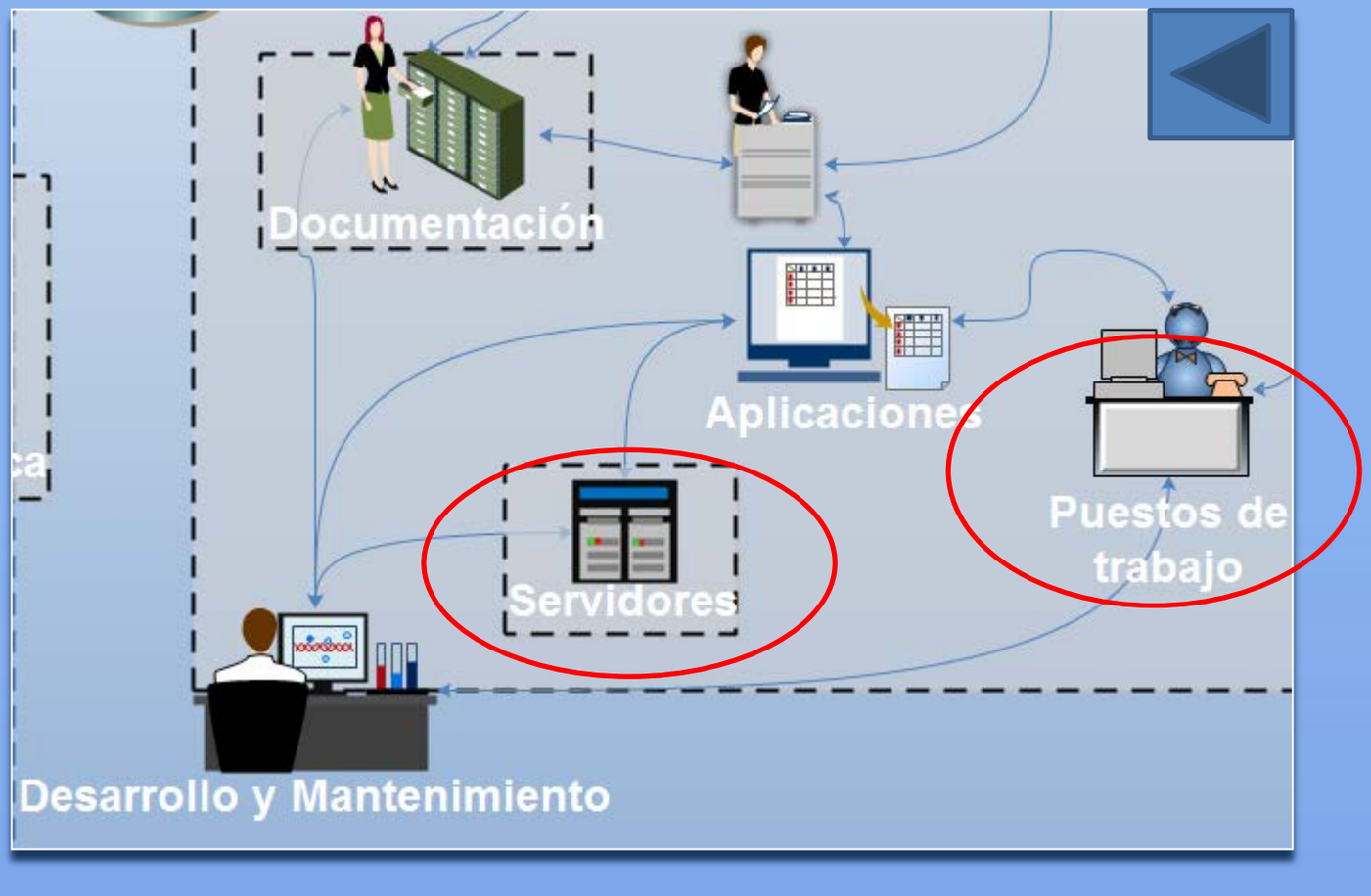
9.2.4 Mantenimiento de equipos

www.iso27002.es



Posibles controles relacionados a tener en cuenta :

9.2.4 Mantenimiento de equipos
10.1 Procedimientos y responsabilidades de operación
10.3. Planificación y aceptación del sistema
10.5 Gestión interna de soportes y recuperación
10.7 Utilización y seguridad de los soportes de información
10.10. Monitorización
12.2 Seguridad de las aplicaciones del sistema
12.4 Seguridad de los ficheros del sistema
12.5. Seguridad en los procesos de desarrollo y soporte
12.6. Gestión de las vulnerabilidades técnicas
13. Gestión de Incidentes de Seguridad de la Información
15.2. Revisiones de la política de seguridad y de la conformidad técnica
15.3. Consideraciones sobre la auditoria de sistemas



Posibles controles relacionados a tener en cuenta:

6.2.1. Identificación de los riesgos derivados del acceso de terceros

9.2 Seguridad de los equipos

10.3 Planificación y aceptación del sistema

10.4 Protección contra software malicioso y código móvil

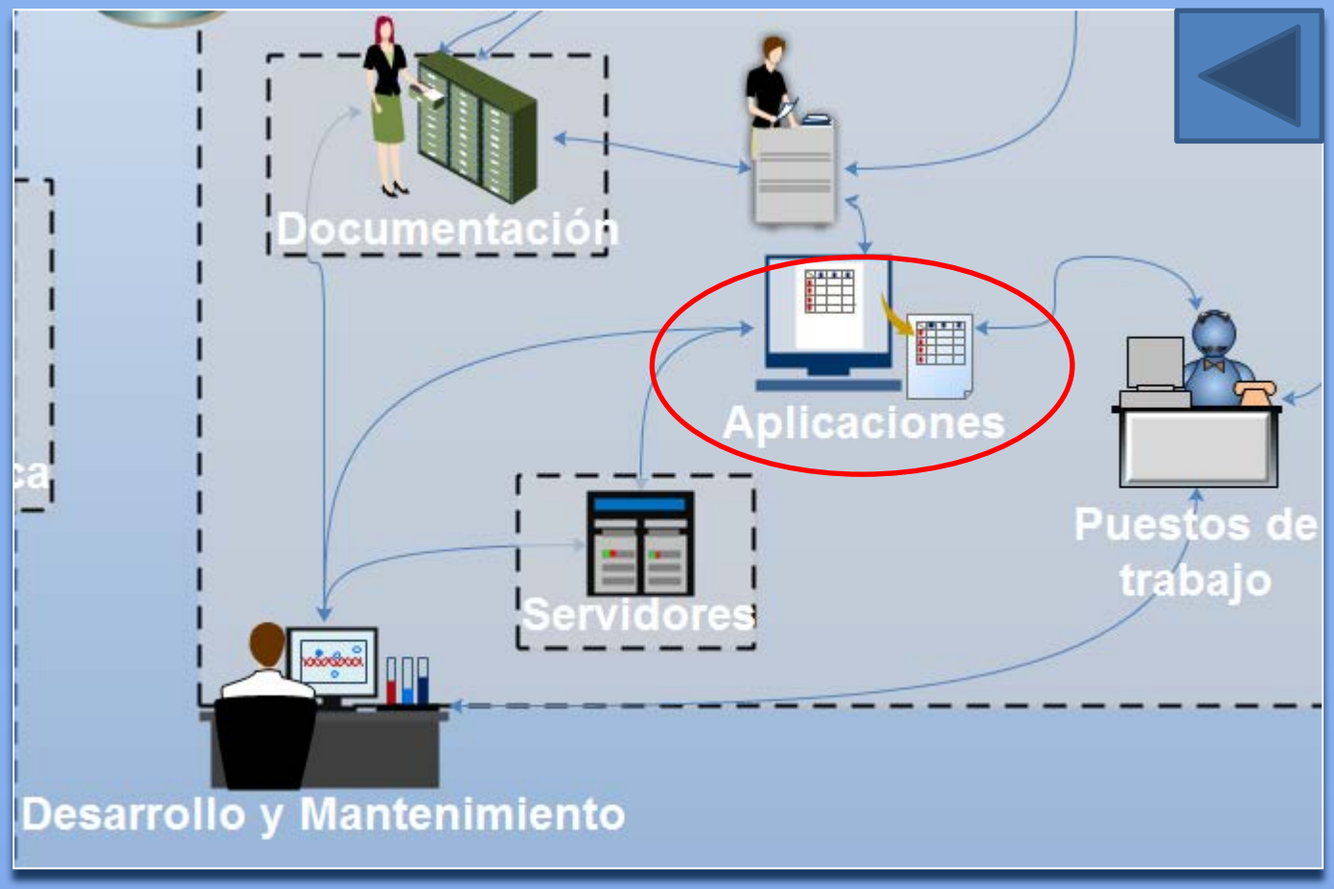
10.10 Monitorización

11.6.2 Aislamiento de sistemas sensibles

11.3.2.Equipo informático de usuario desatendido

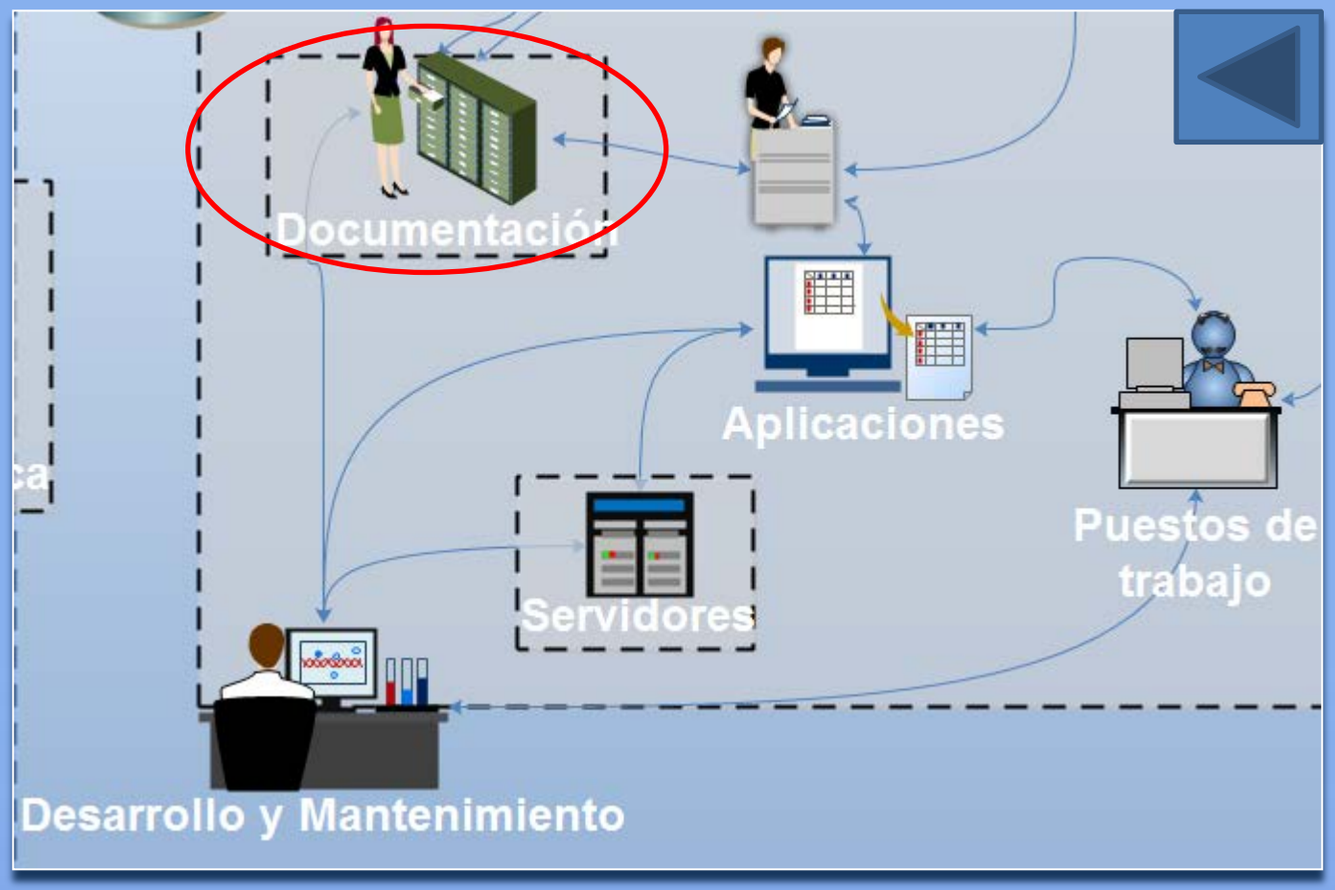
11.3.3 Políticas para escritorios y monitores sin información

www.iso27002.es



Posibles controles relacionados a tener en cuenta :

6.2.2 Tratamiento de la seguridad en la relación con los clientes
10.4 Protección contra software malicioso y código móvil
10.5 Gestión interna de soportes y recuperación
10.8.1 Políticas y procedimientos de intercambio de información y software
10.8.5 Sistemas de información empresariales
10.9 Servicios de comercio electrónico
11.2 Gestión de acceso de usuario
11.5 Control de acceso al sistema operativo
11.6 Control de acceso a las aplicaciones
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
15.3.2 Protección de las herramientas de auditoria de sistemas



Posibles controles relacionados a tener en cuenta:

6.1.5 Acuerdos de confidencialidad
6.2.1 Identificación de los riesgos derivados del acceso de terceros
07. Gestión de Activos
8.3.2 Restitución de activos
9.1 Áreas seguras
9.2.7 Traslado de activos
10.1.1 Documentación de procedimientos operativos
10.5.1 Recuperación de la información
10.7 Utilización y seguridad de los soportes de información
10.8.1 Políticas y procedimientos de intercambio de información y software
10.8.2.Acuerdos de intercambio
11.7.2 Teletrabajo.

www.iso27002.es

Posibles controles relacionados a tener en cuenta:

05. Política de Seguridad

6.1 Organización Interna

07. Gestión de Activos

10.1 Procedimientos y responsabilidades de operación

11.1 Requerimientos de negocio para el control de accesos

12.1 Requisitos de seguridad de los sistemas

12.3 Controles criptográficos

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15.1 Conformidad con los requisitos legales

Posibles controles relacionados a tener en cuenta:

5.1.1 Documento de política de seguridad de la información

08. Seguridad ligada a los Recursos Humanos

10.1 Procedimientos y responsabilidades de operación

11.2 Gestión de acceso de usuario

11.3 Responsabilidades del usuario

13.1 Comunicación de eventos y debilidades en la seguridad de la información