Módulo 4: Tecnologías de la información

Este módulo brinda las pautas y los lineamientos necesarios para que un centro de información pueda contar con una infraestructura tecnológica que le permita garantizar su funcionamiento.

Las características del hardware y software recomendados en este módulo deben ser reevaluadas y actualizadas por el especialista previa su adquisición, debido a la rápida evolución de las tecnologías.

Al final de este módulo conocerá:

- los requerimientos tecnológicos mínimos para garantizar el funcionamiento de un centro de información y la creación de productos y servicios;
- las pautas para dar mantenimiento a los recursos tecnológicos del centro;
- las pautas para dar mantenimiento a las bases de datos que ofrece el Sistema de Gestión de Bases de Datos de la Plataforma de Gestión de Productos y Servicios del Toolkit;
- el procedimiento para realizar el respaldo y la restauración de la información del centro;
- procedimientos de seguridad e integridad de la información.

¿A quién está dirigido?

Este módulo está dirigido a:

- responsables de tecnología;
- responsables de gestión y manejo técnico de la información;
- responsables de la gerencia del centro de información.

Piezas de conocimiento

- ¿Cuáles son los requerimientos tecnológicos mínimos (hardware y software) para crear un centro de información?
- ¿Cuál es el proceso para el mantenimiento de los componentes del centro de información?
- ¿Cuál es el proceso para dar el mantenimiento adecuado a las bases de datos?
- ¿Cuáles son los lineamientos para efectuar copias de respaldo?
- ¿Cómo garantizar la seguridad de la información del centro?

En el centro de información, las principales funciones que cumplen las tecnologías de información son:

- facilitar la creación y el mantenimiento de productos y servicios;
- permitir la prestación de servicios de información a los/as usuarios/as;
- hacer posible el acceso virtual a los servicios del centro de información;
- automatizar procesos técnicos y administrativos en el centro de información.

Antes de empezar

Cuando pase el *mouse* o ratón sobre el símbolo [!], aparecerá la fuente de la que se ha extraído la información. De igual manera, cuando mueva el *mouse* o ratón desaparecerá de inmediato el texto.

A lo largo de este módulo encontrará una serie de íconos a los que debe prestar especial atención. Conozca su significado a continuación:

	**Consideraciones generales** Al hacer clic sobre este ícono, le aparecerá información sobre aspectos que debe tener en cuenta a la hora de desarrollar algunas herramientas. Cuando el ícono aparece junto al título, no le dará la opción de acceder a información adicional pues únicamente facilita la ubicación de este apartado.
	**Requerimientos técnicos/tecnológicos** Al hacer clic sobre este ícono, podrá acceder a información sobre los requisitos técnicos para desarrollar la herramienta a la que se refiera el apartado.
	**Instalación** Al hacer clic sobre este ícono, tendrá acceso a la información relativa a la instalación de la herramienta referida en el apartado.
	**Concepto** Esta pieza aparecerá al lado de conceptos clave que debe aprender.
	**Importante/Recuerde siempre que:** Al lado de este ícono encontrará recomendaciones, advertencias y consejos que debe conocer.
	**Herramienta** Al lado de este ícono encontrará la descripción de herramientas que le serán de utilidad en su centro de información.

Unidad 1. Recursos tecnológicos para la implementación de un centro de información

El servidor, las herramientas de administración de servicios y funciones, las telecomunicaciones y la red local son los cuatro grupos interrelacionados en los que se engloban los recursos tecnológicos mínimos de un centro de información.

En esta unidad se tratarán los siguientes temas:

- Identificación de los recursos de hardware mínimos de un centro de información.
- Programas (software) recomendados para el funcionamiento del centro.
- Los lineamientos para el mantenimiento preventivo de la infraestructura tecnológica.

El servidor

Hardware

Servidor

El servidor es la computadora encargada de almacenar y hacer disponible la información electrónica publicada por el centro.

Este servidor aloja el IIS (*Internet Information Server*), las bases de datos y administra otros componentes importantes (impresoras, *backup*, correo electrónico, etc.). Por ello, el centro debe contar con una computadora para este fin.

Funciones del servidor

- Administrar y controlar el sitio web, incluyendo los productos y servicios que este alberga.
- Administrar los servicios de red que utiliza el centro: administración de impresoras compartidas, acceso a Internet, servicios de archivos, correo electrónico, etc.
- Permite implementar procedimientos para tener la información del centro respaldada.
- Proteger la red de los virus informáticos.
- Administrar el sistema de correo electrónico.

Configuración mínima

Vea el Anexo 1

Software

El servidor debe tener instalado lo siguiente:

- **Sistema operativo**

Microsoft Windows

- En sus diferentes versiones, Microsoft Windows es el sistema operativo más ampliamente usado.
- Es un producto propietario de Microsoft por el que se debe pagar.
- La adquisición del sistema operativo nos brinda el servicio de soporte técnico y actualizaciones por un período limitado (generalmente, de un año) y debe ser renovado al cabo de este plazo. Existen diferentes planes de soporte técnico con diferentes niveles de servicios y costos.
- Windows incluye una herramienta de actualización automática que permite corregir errores y debilidades de seguridad. Sin embargo, la actualización a una nueva versión implica un costo y, usualmente, nuevos términos de licencia.
- Se recomienda utilizar como mínimo el sistema operativo Microsoft Windows Server 2003 Release 2.

Si necesita más información sobre servidores, una visita a la página web de Microsoft le ayudará.

Linux

- Pertenece a una familia de tecnologías de código abierto (open source) que surge como una alternativa a los productos Microsoft.
- Existen distribuciones (“distros”) que se pueden ser adquirir gratuitamente desde la web y distribuciones comerciales que tienen un costo (generalmente, menor que el de los productos de Microsoft).

Distribución de Linux

Una distribución de Linux es una línea de desarrollo del producto elaborada y mantenida por una comunidad de programadores.

Hay gran número de distribuciones distintas de Linux. Cada una tiene un conjunto de herramientas y capacidades que pueden variar de una distribución a otra. Por ejemplo, algunas distribuciones de Linux tienen interfaces de usuarios/as diferentes, algunas están orientadas a tareas específicas como seguridad de la información, la implementación de servidores, etc.

Las comunidades de usuarios/as de Linux mayormente proporcionan el soporte técnico de forma voluntaria. Además, es posible contratar el servicio de soporte de compañías técnicas comerciales. Algunas distribuciones de Linux incluyen herramientas de actualización automática que permiten corregir errores y problemas de seguridad, e incluso, a diferencia de Microsoft Windows, permiten la actualización a nuevas versiones del sistema operativo sin costo adicional.

Sin embargo, normalmente el personal técnico debe estar atento a cambios en el sistema operativo y sus aplicativos básicos y a los efectos de estos en las aplicaciones existentes. Algunas distribuciones requieren actualización manual.

Existe un gran número de distribuciones libres y comerciales que proporcionan las funcionalidades que necesita un servidor, por lo que varias de ellas pueden ser adecuadas. Si necesita más información sobre este punto, acceda a la página web de Distrowatch.

Se recomienda usar las distribuciones libres Ubuntu o Fedora, o la distribución comercial Red Hat.

Nota

La Plataforma de Gestión de Productos y Servicios del Toolkit utiliza algunas aplicaciones desarrolladas por BIREME (Centro Latinoamericano y del Caribe de Información en Ciencias de la Salud) que funcionan tanto en Windows como en Linux.

En resumen, ¿qué diferencias hay entre Linux y Microsoft Windows? En el siguiente cuadro lo podrá observar.

Resumen comparativo de sistemas operativos

Linux	Microsoft Windows
Costo menor.	Costo mayor.
Licencia libre y propietaria. - Las versiones libres no cuentan con el respaldo de una firma comercial. - Las versiones comerciales generalmente cuentan con una responsabilidad limitada de una firma comercial.	Licencia propietaria. - Las versiones cuentan con el respaldo de una firma comercial que garantiza su funcionamiento.
Puede funcionar en servidores que tengan menores recursos tecnológicos (velocidad de proceso, memoria, espacio en disco duro, etc.).	Requiere mayores recursos tecnológicos en el servidor.
Cuenta con comunidades de apoyo que pueden brindar voluntariamente su aporte técnico.	El soporte técnico es comercial.
Existen menos profesionales capacitados/as en esta plataforma.	Hay mayor número de profesionales capacitados/as en el manejo de Microsoft Windows.

- **Software administrador de servicios web**

Internet Information Server (IIS)

- Es un sistema administrador de servicios web propietario de Microsoft que solo trabaja sobre servidores Windows.
- Incluye una interfaz de administración altamente gráfica y de fácil utilización.
- Cuenta con el respaldo técnico y garantía de Microsoft Corporation. Es parte del sistema operativo Microsoft Windows Server. Por lo tanto, su uso no tiene un costo adicional hasta un límite de sitios web hospedados en el servidor (actualmente, 50). Superar el límite implica un costo adicional.

Tenga en cuenta que...

Algunas aplicaciones desarrolladas para ejecutarse en otros sistemas administradores de sitios web podrían no funcionar en IIS.

Si le interesa saber más sobre las características de ISS 7.0, véalas en la página web de Microsoft.

Apache Web Server

- Es un sistema multiplataforma gratuito que puede ser instalado en servidores Windows o Linux.
- Por lo general, la administración de Apache requiere un trabajo más detallado y un nivel mayor de conocimientos técnicos.
- La interfaz de administración no es generalmente gráfica.
- El servidor Apache permite un alto grado de flexibilidad, funcionalidad y rendimiento.
- Debe tener en consideración que algunas aplicaciones desarrolladas para ejecutarse en otros sistemas administradores de sitios Web podrían no funcionar en Apache.

La Plataforma de Gestión de Productos y Servicios del Toolkit utiliza algunas aplicaciones desarrolladas por BIREME (Centro Latinoamericano y del Caribe de Información en Ciencias de la Salud) que funcionan tanto en Windows como en Linux.

El siguiente cuadro le será de utilidad para tener un panorama comparativo claro del software administrador de servicios web.

Resumen comparativo de servidores web

Internet Information Server (IIS)	Apache Web Server
Es un producto comercial.	Es un producto libre.
Funciona solo sobre sistemas operativos de Microsoft Windows.	Funciona en múltiples sistemas operativos tales como Microsoft Windows y Linux.
La instalación es más fácil.	La instalación requiere mayor trabajo y conocimiento.
Cuenta con el soporte técnico de Microsoft Corporation.	Cuenta con el apoyo de las comunidades de programadores y usuarios/as.
Contiene un número determinado de funciones y capacidades.	Ofrece más flexibilidad, funcionalidad y un mejor rendimiento.
La administración se hace mediante una interfaz gráfica de fácil uso.	Usualmente la administración no es gráfica y requiere más trabajo.

Fuente: elaboración propia.

- **Software servidor de correo electrónico**

Servidor de correo electrónico

Un servidor de correo electrónico es un producto de software que permite la habilitación del servicio de correo electrónico.

- Permite una buena administración de la seguridad y privacidad de los correos electrónicos.
- Garantiza la fiabilidad de los datos.
- Incrementa el rendimiento en el proceso de sincronización de mensajes.
- Permite una fácil administración e implementación en el centro.
- Requiere licencia por servidor de usuario/a.
- Es un sistema bajo licencia *open source* que trabaja bajo alta demanda y permite el manejo de múltiples dominios.
- Administra listas de correo, alias, usuarios/as virtuales y tiene un excelente control de acceso.

Se recomienda utilizar un software servidor comercial como Microsoft Exchange Server. Sin embargo, también se puede utilizar un software de acceso libre que permita un nivel básico de administración y control como el software hmailServer que trabaja en Windows, o el programa SendMail para Linux.

A continuación se describirán las características más relevantes de las alternativas mencionadas.

Microsoft Exchange Server

¿Quiere conocer más? Vea sus características en la página web de Microsoft.

HmailServer

Es un sistema libre de costo que trabaja sobre Microsoft Windows, de gran uso por proveedores de servicios Internet.

SendMail

¿Quiere saber más? Revise la Guía de instalación y operación de SendMail en la página www.sendmail.org.

El siguiente cuadro comparativo le puede ayudar a tomar una decisión sobre el software de correo electrónico que empleará en el centro de información.

Resumen comparativo de software de correo electrónico

Microsoft Exchange Server	hmailServer	SendMail
Exclusivo para Microsoft Windows.	Trabaja sobre Microsoft Windows.	Trabaja sobre Linux.
Es un producto comercial.	Es un producto libre.	Es un producto libre.
Cuenta con el soporte técnico de Microsoft Corporation.	Cuenta con el apoyo de las comunidades de programadores y usuarios/as.	Cuenta con el apoyo de las comunidades de programadores y usuarios/as.
Es de fácil instalación y administración.	La instalación es rápida.	La instalación requiere mayor trabajo y conocimiento.

Otras opciones para la administración del correo electrónico

Una opción económica y que no requiere de un servidor instalado es la externalización de los servicios de correo electrónico. Por ejemplo, existen compañías como Gmail versión empresarial y Outlook online que proporcionan este servicio.

- **Software de respaldo**

  El software de respaldo permite administrar y controlar diversas copias de archivos digitales importantes en diversos tipos de dispositivos de almacenamiento (cintas, discos duros externos, etc.). Es efectivo si sigue estrictamente los procedimientos de seguridad y mantenimiento de la información establecidos por la institución.

  CA ArcServer Backup

  - Es un sistema comercial que trabaja sobre plataforma Microsoft Windows y Linux.
  - Permite una gestión centralizada.
  - Mejora el rendimiento y la fiabilidad a través de la integración con cintas de respaldo.
  - Brinda protección contra los virus informáticos incluyendo procesos de encriptación.

  FBackup

  - Es un sistema libre de costo que trabaja sobre plataforma Microsoft Windows.
  - Permite al/a la usuario/a controlar múltiples destinos de copias de respaldo, comprimir la información, generar copias de archivos abiertos y actualizarse en forma automática.

  Clonezilla

  - Es una herramienta para realizar copias de seguridad de nuestros discos duros, independientemente del sistema operativo que contenga.
  - Permite la realización de imágenes de discos y luego restablecerlas en otra computadora.

- **Software firewall**

	**Firewall** El firewall es un filtro de seguridad que controla todas las comunicaciones electrónicas que pasan por una red. Permite o bloquea cierto tráfico de acuerdo con las normas de seguridad establecidas. Este software ayuda, por ejemplo, a evitar el acceso ilícito a los recursos electrónicos del centro (hackers) o el uso indebido de algunos recursos tecnológicos. Este proceso de filtrado se realiza sobre servicios electrónicos como acceso a sitios web, correo electrónico, mensajería instantánea y transferencia de archivos (FTP), entre otros.

ISA Server

- Es un sistema comercial que trabaja sobre plataforma Microsoft Windows.
- Protege los sistemas de amenazas procedentes de Internet permitiendo a los/as usuarios/as acceder en forma remota y segura a sus aplicaciones y datos corporativos.
- Existen dos versiones: ISA Server Edición Estándar e ISA Server Edición Enterprise.

Comodo

- Es un sistema libre de costo que trabaja sobre plataforma Linux.
- Permite proteger nuestro sistema ante ataques de virus informáticos, troyanos, hackers y otros, controlando en detalle las aplicaciones que tienen acceso a Internet a través de reglas de acceso y del monitoreo constante de su comportamiento.

- **Software antivirus**

	**Antivirus** El antivirus es un software que se encarga de detectar, detener y eliminar la mayor cantidad de amenazas de virus informáticos que puedan afectar el servidor. Para ello, monitorea permanentemente todos los archivos abiertos, creados, modificados, ejecutados y transmitidos mientras el servidor trabaja.

ESET NOD32

- Es un sistema comercial que trabaja sobre plataforma Microsoft Windows.
- Permite analizar los archivos a gran velocidad con una alta tasa de detección de virus informáticos.
- Optimiza el consumo de los recursos del servidor y brinda la posibilidad de analizar archivos en formato comprimido (ZIP, RAR, ARJ, LZH, LHA, CAB, CHM, TAG, GZIP).

Bastille

- Es un sistema gratuito que trabaja sobre plataforma Linux.
- Permite:
- deshabilitar los protocolos de acceso remoto.establecer periodos de caducidad para las contraseñas;
- deshabilitar las teclas Ctrl-Alt-Supr para evitar reiniciar el servidor limitar el uso de los recursos del sistemas;
- guardar un historial de todos los comandos ejecutados por cada usuario/a.

- **Software de monitoreo de la red**
  - El sistema de monitoreo de la red nos permite visualizar la actividad en la red.
  - Identifica las computadoras y periféricos conectados, la disponibilidad y rendimiento de la red y los protocolos de comunicación (HTTP, SMTP, FTP, DNS, POP3, etc.) utilizados en la red.
  - Genera estadísticas útiles de los dispositivos y actividades detectados.

AWSTATS

- Es una herramienta libre disponible bajo la licencia pública general GNU.
- Trabaja tanto sobre plataforma Microsoft Windows como en Linux. En ambos casos necesita tener instalado previamente el Perl.
- Genera diversos tipos de cuadros estadísticos y gráficos que permiten analizar el uso de la red.
- Genera reportes sobre el uso de determinadas aplicaciones tales como número de visitas al sitio web, procedencia de los/as usuarios/as de los servicios electrónicos, tipos de aplicaciones utilizadas, etc.

Herramientas de administración de servicios y funciones

- ## Software

Productos de software mínimos de un centro de información

Sistema operativo Microsoft o Linux

En sus diferentes versiones para computadoras personales, Microsoft Windows es el sistema operativo comercial más ampliamente usado.

Windows XP cuenta con un servicio automático gratuito de actualizaciones a través de Internet que ayuda a mantener este sistema operativo actualizado.

Sistema antivirus

- **ESET NOD32** es un sistema antivirus comercial que trabaja sobre plataforma Microsoft Windows.
- **Avast! Linux home Edition** es un sistema antivirus para Linux que se ofrece con licencia libre para uso no comercial.

Software cliente de correo electrónico

- **Outlook Express** de Microsoft Windows es el programa que viene incluido en el Microsoft Internet Explorer a partir de la versión 4.
- **Zimbra** es la solución libre para correo electrónico y calendario de código abierto para empresas instituciones, etc.

Software para diseño gráfico

El software para diseño gráfico permite el manejo de imágenes en diferentes formatos digitales para ayudar al centro en la creación y mejora de logotipos, banners, fotografías y otros materiales gráficos para publicaciones y sitios web.

Se recomiendan los siguientes productos:

- **GIMP** (GNU, *Image Manipulation Program*) es una aplicación libre de costo orientada a la manipulación de imágenes. Trabaja sobre las plataformas Microsoft Windows y Linux.
- **Photoshop** de Adobe es el producto comercial manejador de gráficos más popular y cuenta con el mayor surtido de funciones gráficas.

Software para edición de páginas web

Este software se utiliza para la creación y edición de páginas web.

Se recomiendan los siguientes productos:

- **KompoZer**
  - Es un editor web gratuito para lenguaje HTML basado en el popular NVU (editor WYSIWYG multiplataforma construido sobre Mozilla Composer).
  - Permite a usuarios/as sin conocimiento alguno de programación crear su propia página web partiendo desde cero mediante la simple introducción de diversos elementos (botones, imágenes, tablas, formulario, etc.) en el entorno (página web).
  - La interfaz del programa se encuentra bien estructurada, y permite al usuario ver en cualquier momento el resultado final de la web en construcción y el código HTML generado por KompoZer.

- **Dreamweaver**
  - Es un editor comercial de Adobe disponible para Windows.
  - Ofrece más funciones para la creación, edición y publicación de páginas web.

Software de edición de documentos MS Office u Open Office

- **MS Office**. Microsoft Office es una suite de oficina que abarca e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows y Mac OS X.
- **OpenOffice**. OpenOffice.org (frecuentemente escrito OOo) es una suite ofimática libre (código abierto y distribución gratuita) que incluye herramientas como procesador de textos, hoja de cálculo, presentaciones, herramientas para el dibujo vectorial y base de datos.

- **Hardware**

Computadora

Es la herramienta utilizada por el personal del centro para realizar las funciones administrativas y de servicios del centro.

Funciones:

- Apoyar las actividades de gestión de información (registro en bases de datos, digitalización, uso de Internet y aplicaciones web, edición de documentos, etc.).
- Permitir que el/la gestor/a de información y el resto del equipo del centro puedan llevar a cabo sus tareas.
- Facilitar la comunicación del centro con sus usuarios/as.

Configuración mínima

Vea el Anexo 2

Impresora

Las impresoras son equipos cuya finalidad es la de reproducir en papel los textos o gráficos de los diversos documentos almacenados en formato electrónico. Principalmente se busca calidad y rapidez en el proceso de impresión.

Características mínimas

Vea el Anexo 3

Escáner

El escáner es un equipo diseñado para capturar en forma óptica las imágenes o textos de documentos y llevarlos a un formato digital para ser procesados en una computadora.

Características mínimas

Vea el Anexo 4

Fotocopiadora

Características mínimas

Vea el Anexo 4

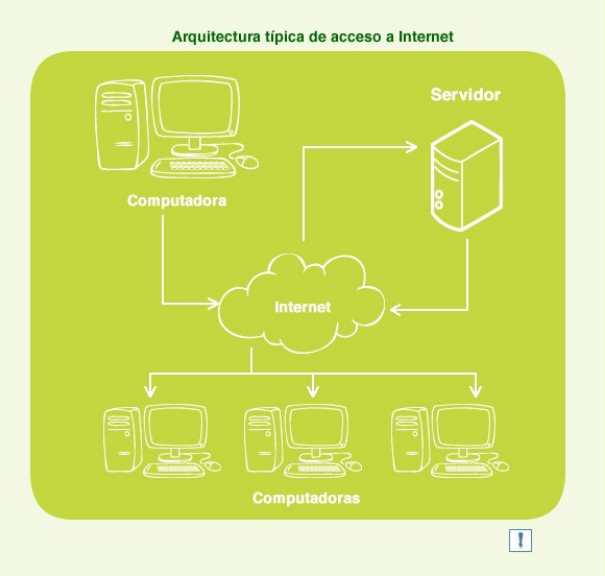
Telecomunicaciones

Recursos de telecomunicaciones mínimos de un centro de información

Servicio de Internet

Es el enlace de alta velocidad que proporciona al centro de información acceso a Internet. Este servicio implica tener un contrato de servicios con una empresa proveedora de servicios Internet (ISP). Existen diferentes tecnologías que permiten esta conexión: ISDN, fibra óptica, ADSL, wireless, cable y otros.

Al contratar un servicio, se debería adquirir el mejor tipo de tecnología que su proveedor ofrezca, con una velocidad mínima de 1 Megabit por segundo (Mbps). Es preferible que el proveedor proporcione todo el equipo necesario para conectar la red local del centro al Internet (incluyendo el módem y su configuración) y el soporte técnico.



Fuente: elaboración propia.

Router

Router

El router es el dispositivo que permite administrar el tráfico de datos entre la red local y el Internet; se encarga de garantizar que las comunicaciones lleguen al destinatario correcto. Además, puede realizar algunas tareas de seguridad de las comunicaciones.

Características mínimas

Vea el Anexo 6

Se recomienda por ejemplo un router de cable/ADSL EtherFast con conmutador de cuatro puertos modelo BEFSR41 de Linksys.

Línea telefónica

La línea telefónica se requiere para el uso del fax y para la comunicación de voz. El centro de información debe contar como mínimo con un teléfono.

Router inanalámbrico

El router inalámbrico (*wireless*) provee la conexión inalámbrica a Internet y el acceso a los recursos de red. Es útil cuando se utilizan computadoras portátiles (laptop) y dispositivos portátiles como celulares, PDA, etc.

Red local

La red local debe contar como mínimo con:

Cableado de red

El cableado de red permite la comunicación entre los equipos de cómputo para el intercambio de información. Generalmente, las redes locales emplean cable de par trenzado.

Se recomienda usar como mínimo el cable Ethernet de par trenzado categoría 5E y que la instalación cumpla con las normas internacionales de cableado estructurado. Es importante que se considere cableado redundante para prevenir problemas por fallas de conexión.

Puede profundizar en este tema visitando Ethernet and UTP Cabling from 10BASE-T to 10GBASE-T.

Switch Ethernet

El Switch Ethernet es un elemento de la red local que hace posible la conectividad de la red mediante el sistema de cableado. Se recomienda como mínimo utilizar un switch de ocho puertos.

¿Necesita saber más sobre este punto? Revise la página web de Cisco Systems.

Cierre de unidad 1

Recapitulando...

Ya finalizada la unidad 1, se puede proceder a su repaso.

En esta unidad se han presentado los recursos tecnológicos necesarios para desarrollar un centro de información. Los recursos tecnológicos se clasifican en cuatro grandes grupos interrelacionados entre sí: el servidor (debe tener instalado el sistema operativo, un software para administrar los servicios web, un software servidor de correo electrónico, un software de respaldo, un software firewall, un software antivirus y un software de monitoreo de uso), las herramientas de administración de servicios y funciones (equipos de hardware y software mínimos recomendados para un centro de información), telecomunicaciones (router, línea telefónica y servicio de Internet) y red local (cableado de red y Switch Ethernet).

En anexos se han señalado marcas que cumplen con los requerimientos mínimos. Sin embargo, recuerde que existen numerosas marcas en el mercado, y es responsabilidad exclusiva del personal de tecnología elegir el modelo y la marca que mejor cumpla con los requerimientos de su centro.

Recomendamos visitar

Servidores

Hardware

DELL. Servidor PowerEdge R200 Rack Server

Hewlett-Packard. Servidor modelo HP ProLiant DL120 G5 Server

Software

Microsoft Windows Server 2003 Release 2

Linux UBUNTU

Linux FEDORA

Servidores web

Microsoft Internet Information Server 6.0

Apache Web Server

Servidores de correo electrónico

Microsoft Exchange Server

hMailServer

SendMail

Sistemas de respaldo

CA ArcServer Backup

FBackup

Sistemas firewall

Microsoft ISA Server

Comodo

Sistemas antivirus

ESET NOD32

Bastille

Sistemas de monitoreo

AWSTATS

Equipos para el centro de información

Computadora personal

Hardware: DELL Modelo Optiplex 760

Sistema operativo: Microsoft Windows XP

Sistema antivirus: ESET NOD 32

Sistemas firewall:

- Zone Alarm
- Comodo

Sistema cliente de correo electrónico: Microsoft Outlook Express

Sistema para diseño gráfico: GIMP

Sistema para edición de páginas web: KompoZer

Impresora

Hewlett-Packard modelo HP Office Jet H470

Módem

Telecomunicaciones

Router

Red local

El cableado de red

Otros documentos sobre cableado de red

Archivo comprimido con varios documentos de interés sobre el tema.

Switch Ethernet

Bibliografía (en anexo)

Unidad 2. Funciones de gestión de las tecnologías de información

- Tareas de gestión de tecnologías de información
- Estrategias y lineamientos para la seguridad de la información
- Cierre de unidad

En la unidad anterior ha comprobado la importancia de contar con una buena infraestructura tecnológica para optimizar el rendimiento de los servicios del centro de información hacia sus usuarios/as. En esta unidad verá que establecer los mecanismos de seguridad y de mantenimiento de la plataforma tecnológica es una actividad crítica e importante porque le permitirá garantizar la operatividad de los productos y servicios.

Tareas de gestión de tecnologías de información

Definición de procedimientos y reglas de funcionamiento

El profesional de tecnología de información es el responsable de esta tarea, y seguirá las directrices que emanan de la dirección del centro.

Los procedimientos y reglas a definir incluyen lo siguiente:

- Normas de seguridad: por ejemplo, definir niveles de acceso y seguridad de los recursos informáticos a su cargo.
- Reglas de mantenimiento de hardware y software: por ejemplo, frecuencia de actualización de software y equipamiento.
- Procedimientos de respaldo: por ejemplo, frecuencia y tipo de respaldo de datos.
- Directivas de documentación: por ejemplo, pasos para documentar nuevos productos desarrollados por el centro.
- Normas de almacenaje e inventario de recursos informáticos: por ejemplo, cómo mantener actualizado el estado de materiales y equipos de centros de cómputo.
- Procedimientos de reporte para la gerencia: por ejemplo, con qué regularidad se entregan reportes de uso de los servicios electrónicos a la gerencia.

Estos procedimientos y reglas deben ser actualizados con regularidad o cuando sea necesario.

Diseño e implementación de soluciones tecnológicas

Esta tarea abarca las actividades necesarias para crear herramientas tecnológicas que resuelvan nuevas necesidades del centro de información. Por ejemplo, diseñar e implementar un nuevo producto de software, diseñar y adquirir equipamiento que permita procesar nuevos tipos de información, etc.

Gestión de la seguridad y mantenimiento de las tecnologías de información

Las actividades de seguridad y mantenimiento de las tecnologías son vitales y permanentes. Estas actividades deben tomar en cuenta los procedimientos y reglas definidas y las mejores prácticas profesionales posibles. Si desea más detalles de este tema, vaya a la sección 2.2 Estrategias y lineamientos para la seguridad y mantenimiento de la información de esta unidad.

Monitoreo del estado y uso de los recursos tecnológicos

Esta tarea involucra la observación permanente del funcionamiento y uso de los recursos tecnológicos. Esta observación requiere la generación de informes para mantener un registro de los eventos.

Actualización de tecnologías

Estas actividades involucran la investigación de nuevas tendencias tecnológicas para actualizar los recursos del centro a fin de mantener un nivel de servicios y eficiencia funcional acorde con las expectativas y requerimientos de los/as usuarios/as y de la misma organización.

Estrategias y lineamientos para la seguridad de la información

Los puntos arriba citados son los objetivos de las estrategias para la seguridad de la información. Estas deben definir políticas, controles de seguridad, tecnologías y procedimientos que permitan detectar cualquier tipo de amenaza.

La seguridad de la información garantiza la confidencialidad, integridad y disponibilidad de la información. ¿De qué se trata?

- La **confidencialidad** se refiere a mantener la información privada fuera del acceso de personas o procesos no autorizados.
- La **integridad** es la propiedad de controlar que la información no sea modificada cuando no se desea.
- La **disponibilidad** consiste en que las personas autorizadas tengan disponible la información a la que se les ha dado acceso.

Este ejemplo puede ser muy gráfico:

Si alguien roba un activo de información (computadora, informe, disco compacto, etc.), una persona no autorizada podría leer y difundir la información contenida. Desde esta situación podemos decir:

Está en peligro la confidencialidad de la información.

Si la persona no autorizada corrompe, modifica o borra la información contenida, la integridad de la información se vería comprometida.

Finalmente, si esa información no fue respaldada en otro soporte, podría haber problemas de disponibilidad, dado que ninguna persona tendría acceso a esta información.

Concientizar a los/as usuarios/as sobre los aspectos de seguridad de la información

Es fundamental entrenar y concientizar al personal del centro sobre los aspectos de seguridad de la información. El personal del centro debe involucrarse y asumir un rol protagónico y responsable como parte de un sistema integral de seguridad.

Deben existir políticas de formación clara, concisas y permanentes orientadas a formar a los/as empleados/as del centro sobre los siguientes aspectos:

- Entender los tipos de riesgos de seguridad de los recursos informáticos y su implicación en el desempeño del centro.
- Lineamientos para realizar los respaldos de información.
- Buenas prácticas en el manejo y conservación de los soportes informáticos (dispositivos USB, discos compactos, DVD, etc.).
- Manejo del correo electrónico.
- Normas para el intercambio de información.
- Principios de comportamiento ético profesional que guíen a los/as empleados/as en sus decisiones en el manejo y utilización de los recursos informáticos.

Para profundizar en este tema, le proponemos los siguientes artículos de Internet:

- La Seguridad de la Información en los Recursos Humanos (I)
- El factor humano: el mayor riesgo para la seguridad informática
- El factor humano

Definir los perfiles para los/as usuarios/as

Al definir los perfiles de los/as usuarios/as se asignan diferentes permisos de acceso de acuerdo con las funciones y responsabilidades que cumple el personal del centro.

¿Cómo establecer los diferentes niveles de acceso en un centro de información? Puede seguir los pasos que se indican en el Anexo 7.

Reforzar la seguridad de los sistemas

Garantizar la seguridad de los sistemas en la red de datos permite el buen funcionamiento tecnológico de todo el centro de información. Para ello se recomienda utilizar como mínimo los siguientes mecanismos de seguridad:

Listas de acceso

Es el conjunto de reglas que permiten o prohíben cierto tipo de tráfico en la red. Esto permite controlar diferentes aplicaciones y servicios ofrecidos a través de la red y quiénes están autorizados a acceder a ellos. Estas listas de acceso pueden ser implementadas en el firewall o en el router.

Para definir las listas de acceso considere:

- Usar una lista de acceso por protocolo y por dirección.
- Las sentencias se procesan en forma secuencial desde el principio hasta el final de la lista buscando una concordancia; si no se encuentra ninguna, se rechaza el paquete.
- Existe un “deny any” (denegar cualquiera) implícito al final de todas las listas de acceso.

- Las entradas de la lista de acceso deben establecer un filtro desde lo particular hasta lo general.
- Documentar la lógica de cada una de las sentencias de la lista.
- Las listas de acceso están diseñadas para filtrar el tráfico que pasa por el router más no el tráfico que se origina en el router.

En los siguientes artículos de Internet encontrará más información sobre listas de acceso:

- Uso de listas de acceso en entornos Cisco
- Básicos de Networking. Listas de acceso

Traductor de direcciones de red (*Network Address Translation*-NAT)

El traductor de direcciones de red (NAT) permite el intercambio de paquetes de datos entre dos redes diferentes que se asignan mutuamente direcciones incompatibles.

El NAT le puede ayudar a:

- Mejorar la seguridad al presentarse al exterior como una única máquina permitiéndole concentrar un importante esfuerzo de seguridad en dicho punto.
- Superar el problema de la escasez de direcciones al permitir que múltiples usuarios/as se conecten a la red compartiendo una única dirección IP.
- Simplificar la gestión de redes al permitir migrar redes de forma transparente a los/as usuarios/as finales.

Si le interesa profundizar en este tema, los siguientes artículos de Internet le pueden resultar de utilidad:

- Configuración avanzada puertos NAT
- Accediendo a Configuración de red NAT

Firewall

El firewall es un filtro de seguridad ubicado entre la red local y la red Internet que permite controlar las comunicaciones que pasan de una red a otra utilizando políticas de seguridad, monitoreos y puntos de control. Puede ser un equipo que se conecta entre la red y el cable de conexión a Internet (hardware) o un programa que se instala en una computadora que incluye un módem que se conecta con Internet (software).

<table>
<tr>
<td>  </td>
<td>Tenga en cuenta que...

El firewall no puede proteger la red ante las siguientes situaciones:

• Ataques de fuentes externas o de los/as usuarios/as internos.
• Ataques provenientes de programas maliciosos ejecutados casualmente o intencionalmente en un computador dentro de la red (por ejemplo, archivos de programas recibidos adjuntos en correos electrónicos).</td>
</tr>
</table>

Para obtener mayor información, puede revisar en Internet:

- Componentes y ventajas de un firewall distribuido
- Cómo elegir un firewall
- Tutorial de filtrado de paquetes en redes con iptables

Redes inalámbricas

Si el centro desea habilitar una red de acceso inalámbrico (Wi-Fi), debe establecer los mecanismos de seguridad necesarios para asegurar la privacidad de la red de datos.

Para ello se recomienda:

- **Conectar la red utilizando Wired Equivalent Privacy (WEP)**. La mayoría de redes disponen de encriptación WEP de 64 bits y por lo general los access points tienen el servicio WEP desconectado. Una vez instalado debe activarlos siguiendo el manual de configuración de su equipo. Se recomienda cambiar la clave de acceso a la red Wi-Fi al menos cada dos semanas o incrementar la encriptación a 128 bits haciendo la clave de acceso más compleja.
- **Cerrar la red**. De ser posible, bloquear el Service Set Identifier (SSI) logrando que la red Wi-Fi permanezca oculta reduciendo las oportunidades de ataque de los hackers.
- **Asignar un nombre de red que no identifique a la institución**. Si se elige usar un nombre de red (SSI), se recomienda utilizar uno que no identifique a la organización. Por ejemplo, el nombre puede ser una combinación arbitraria de letras y números.
- **Usar tablas de control de acceso por identificador MAC**. Haciendo uso de las direcciones MAC (Medium Access Control) de las computadoras, se puede limitar las conexiones inalámbricas solo a los equipos cuyas direcciones MAC estén registradas en la lista de control de acceso.
- **Usar una Virtual Private Network (VPN)**. La VPN permite un acceso remoto seguro de una computadora autorizada a través del firewall a la red interna de la organización. Con eso se crean mecanismos de seguridad muy altos para evitar conexiones no autorizadas a la red interna y permitiendo, sin embargo, el acceso remoto de computadoras autorizadas.

¿Necesita más información? Si es así, revisar los siguientes artículos en Internet puede ser de utilidad:

- Seguridad en redes Wi-Fi inalámbricas
- Seguridad en redes Inalámbricas. Una guía básica
- Configuración de redes inalámbricas IEEE 802.11 de Windows XP para el hogar y la pequeña empresa

Efectuar copias de respaldos de la información

Copias de respaldo o *backups*

Las copias de respaldo (*backups*) son copias parciales o totales de información en otro sistema de almacenamiento masivo como son los discos duros externos, CD-ROM, DVD o cintas magnéticas.

En el Módulo 2. Unidad 2. Soportes de almacenamiento, encontrará más información sobre este tema.

Importante

Los *backups* deben guardarse en un lugar seguro, preferentemente en una zona externa al centro de información. Con ellos se garantiza la recuperación de la información en caso de pérdida de datos, de un fallo en el sistema o en la bases de datos, de efectos adversos producidos por los virus informáticos, de problemas de hardware y de catástrofes imprevisibles.

Para efectuar los backups correctamente, tiene que identificar qué datos se deben proteger (ficheros, bases de datos, imágenes, archivos de configuración, etc.). En el caso de un centro de información, al menos deberían ser los siguientes:

- Bases de datos
- Sitio web del centro
- Colección de recursos de información
- Correo electrónico
- Archivos de trabajo de acuerdo a su importancia

Existen diferentes procedimientos para realizar el proceso de *backup* de la información.

Tipos de *backups*

Tipo 1. *Backup* completo

Se crea una copia de respaldo de todos los archivos y carpetas del servidor. El proceso consume mucho tiempo y soporte de almacenamiento pero garantiza la disponibilidad de todos los archivos.

Tipo 2. *Backup* incremental

Crea copias de aquellos archivos que hayan sido modificados o creados después del último backup. Este proceso se basa en la fecha de creación de los archivos y la primera vez que se ejecute realiza un respaldo completo.

Tipo 3. *Backup* diferencial

Este tipo de backup funciona de forma similar al backup incremental, pero comparando efectivamente el contenido de los archivos. Solo copia aquellos archivos nuevos o modificados.

Estrategias y lineamientos para realizar los respaldos

No olvide definir una estrategia de los respaldos que le garantice su correcto funcionamiento en el momento en que se requiera. ¿Qué debe hacer?

- Establecer un horario en el que se realizará el proceso (se recomienda que se realice cuando menos usuarios/as estén trabajando en la red) y el lugar donde se almacenarán las copias de respaldo.
- Realizar revisiones periódicas del soporte de almacenamiento y de la información que se respalda.
- Es conveniente efectuar “simulacros” de restauración de los archivos almacenados en las copias de respaldo.

Revise en el Anexo 8 algunas recomendaciones para realizar los respaldos.

Llevar a cabo un mantenimiento preventivo de los recursos tecnológicos

El mantenimiento preventivo de los recursos tecnológicos involucra un control y seguimiento permanente del estado de los equipos (hardware) y de los sistemas (software) que funcionan en estos para garantizar un buen funcionamiento del centro de información.

Mantenimiento preventivo de hardware

El mantenimiento preventivo de los equipos tecnológicos de un centro de información le permite anticiparse a un eventual problema en su funcionamiento cuya reparación puede resultarle muy costosa a largo plazo. Factores como el polvo, la humedad u otras condiciones ambientales inadecuadas contribuyen al deterioro de los equipos del centro.

Se recomienda realizar mantenimiento preventivo al menos dos veces al año.

En el servidor y estaciones de trabajo

- Explorar periódicamente el disco duro para detectar errores en sus sectores.
- Efectuar una limpieza completa de los componentes y unidades del equipo.
- Ajustar y verificar todas las interfaces de comunicación utilizadas por los equipos. Verificar en todas las unidades de disco el estado de su superficie, el formato del disco y el espacio utilizado.
- Limpiar todos los contactos de las tarjetas y partes externas de los equipos y sus periféricos.
- Verificar el buen estado de los bancos de memoria de los equipos.
- Validar el buen estado de la fuente de poder, cables y conectores. Limpiar internamente todas unidades de USB, CD, DVD.

En impresoras, fotocopiadora y escáner

Para estos equipos se definen dos tipos de mantenimiento preventivo:

- **Operativo**: orientado a mantener limpia la superficie externa del equipo y al cambio cuidadoso de los cartuchos del tóner y tinta.
- **Interno** (realizado por un especialista): consiste en la limpieza y engrasado de todas las piezas internas del equipo.

En caso de que necesite más información, en la página web del CRID cuenta con un artículo sobre mantenimiento preventivo.

Mantenimiento preventivo de software

Sistema operativo

- Mantener actualizado el sistema operativo para optimizar el rendimiento del equipo y reducir las vulnerabilidades.
- Explorar periódicamente el disco duro para detectar errores en sus sectores.
- Efectuar una limpieza de archivos: eliminar todos los archivos temporales generados por el sistema operativo, eliminar los accesos inválidos al registro del sistema así como los accesos directos dañados.
- Desfragmentar el disco duro, lo que permitirá organizar los archivos y una mayor velocidad de acceso a estos.
- Monitorear el sistema para identificar qué aplicaciones necesitan actualizaciones y cómo se están comportando en el sistema.
- Revisar periódicamente la disponibilidad de nuevas actualizaciones del sistema operativo y otros software básicos (se recomienda configurar el sistema para que alerte automáticamente de nuevas actualizaciones).

Sistema antivirus

En la actualidad, es imprescindible contar con un sistema antivirus y mantenerlo actualizado. Este sistema protegerá al computador y a toda la red de los virus que se filtran a través de diferentes aplicaciones.

Se recomienda configurar la actualización automática para que se instalen las nuevas definiciones de virus y otras amenazas y revisar mensualmente la existencia de nuevas versiones de software.

Mantenimiento básico de aplicaciones

Se recomienda efectuar periódicamente los siguientes procesos:

Mantenimiento de la plataforma de bases de datos

- Realizar copias de respaldo de las bases de datos.
- Actualizar el software de la base de datos.
- Revisar la integridad de los archivos de base de datos semanalmente y cada vez que se hagan actualizaciones.

Mantenimiento de la plataforma web

- Revisar la disponibilidad de nuevas versiones del software (Apache, IIS, PHP, etc.). Se debe probar la compatibilidad de nuevas versiones con las aplicaciones usadas por el centro antes de instalar el nuevo software.
- Comprobar que el despliegue del sitio web sea correcto en diferentes monitores, teniendo en cuenta la resolución, colores y formatos de la información desplegada. Asegurar que el sitio web cumpla los estándares de accesibilidad y usabilidad tales como WC3. Se recomienda verificar cada vez que se haga un cambio en el sitio web.
- Probar que el sitio web se visualice bien en varios navegadores como Internet Explorer, Firefox, Safari y otros.
- Verificar por lo menos una vez por semana que funcionen los enlaces del sitio web, incluyendo aquellos relacionados con los servicios internos y enlaces a sitios externos.
- Programar *backups* del sitio web y de las bases de datos que se ejecuten automáticamente y más de una vez por semana. Es importante hacer los respaldos en medios externos (USB, DVD…) o en otro disco.
- Tener una copia local del sitio web y gestionar la publicación del sitio web a través de un hosting o alojamiento externo.

Mantenimiento de la plataforma de correo electrónico

- Asegurar el correcto funcionamiento del software de correo realizando pruebas semanales.
- Verificar la disponibilidad de nuevas versiones de software de correo.
- Respaldar los archivos y bases de datos de correo electrónico usados por el software al menos una vez a la semana.

“Mantenimiento de software” es un artículo que le puede interesar. Se encuentra disponible en la página web de Wikipedia.

Brindar seguridad física a los recursos tecnológicos

Es importante garantizar la seguridad física de los recursos tecnológicos utilizados en el centro de información, en especial, del área de servidores. Aquí debe considerar:

- El buen estado de las conexiones eléctricas. Debe incluir una conexión a tierra para dirigir la energía perdida a la tierra y reducir el riesgo de descargas eléctricas en caso de fallas.
- Un equipo de aire acondicionado que permita mantener en una temperatura óptima los recursos tecnológicos ante el calentamiento natural producido por el permanente trabajo de sus dispositivos electrónicos.
- La implementación de un sistema contra incendios que permita combatir el fuego en su inicio. Puede ser mediante el uso de extintores portátiles (menos de 30 kg) de dióxido de carbono. Se debe verificar su ubicación, tipo, capacidad, carga, fecha de vencimiento, seguro, etiqueta, etc. Hay que saber utilizarlos y seguir el programa de mantenimiento de recarga.
- El tratamiento adecuado del problema acústico y de las vibraciones generadas por las impresoras, el aire acondicionado o cualquier equipo sujeto a grandes vibraciones.
- Un control de acceso del personal que debe permitir identificar claramente quién ingresa y quién sale.
- El uso de sistemas de seguridad como monitores, cámaras y sistemas de circuito cerrado, principalmente en los puntos de entrada y salida.

- El montaje del piso falso que permite transportar la electricidad estática a través de todo el sistema evitando que las descargas provoquen daños progresivos en los equipos de cómputo. También permite una mejor distribución del cableado, canaletas, aire acondicionado y, en general, de todo tipo de cables e instalaciones que no deben estar expuestos al tráfico del personal.
- Muebles técnicos adecuados que permitan una buena organización, distribución y acceso a los diferentes recursos tecnológicos.

Adicionalmente, debe considerar un espacio privado y seguro donde se almacene organizada toda la información que permita garantizar el funcionamiento de los recursos tecnológicos del centro:

- Los manuales de procedimientos y funciones.
- Los manuales de uso y configuración por cada equipo y sistema instalado.
- Los CD-ROM, DVD y disquetes de instalación de los diferentes equipos y sistemas utilizados en el centro.
- Los certificados de garantía, etc.

Si desea ampliar la información, los siguientes documentos pueden ayudarle:

- Estándares sobre Diseño y Estándares sobre Diseño y Funcionamiento de Data Center
- Definición de aspectos eléctricos (UPS y Grupo Generador) a ser tomados en cuenta al momento de diseñar un Centro de Datos (CPD) y su resumen Consideraciones necesarias para el diseño de un Centro de Proceso de Datos (CPD)

Cierre de unidad 2

Recapitulando...

En esta unidad que recién ha finalizado, se ha insistido en la importancia de la seguridad y el mantenimiento de la plataforma tecnológica y de los productos y servicios del centro de información. Se ha indicado cuáles son las tareas de gestión de las tecnologías: definir procedimientos y reglas de funcionamiento; diseñar e implementar soluciones tecnológicas; gestionar la seguridad y el mantenimiento de las tecnologías de información; monitorear el estado y el uso de los recursos tecnológicos; y actualizar las tecnologías.

Recuerde que la seguridad de la información garantiza la confidencialidad, integridad y disponibilidad de la información. Tampoco olvide que las estrategias para la seguridad de la información deben definir políticas, controles de seguridad, tecnologías y procedimientos que permitan detectar cualquier tipo de amenaza. Con ello se concientiza a los/as usuarios/as sobre los aspectos de seguridad de la información; se definen los perfiles para los/as usuarios/as; se refuerza la seguridad de los sistemas; se efectúan respaldos de la información; se lleva a cabo un mantenimiento preventivo de los recursos tecnológicos (hardware, software, aplicaciones y plataforma de correo electrónico); y se les brinda seguridad física.

Recomendamos visitar

Educar a los/as usuarios/as sobre los aspectos de seguridad de la información

RHM Grupo de comunicación. La Seguridad de la Información en los Recursos Humanos

El factor humano: el mayor riesgo para la seguridad informática

IP Comunicaciones. El factor humano es esencial para la seguridad informática

El factor humano

Reforzar la seguridad de los sistemas

Listas de acceso

Uso de listas de acceso en entornos CISCO

Principios Básicos de Networking

Traductor de direcciones de red (NAT)

Qué ventajas tiene Compartir una Carpeta en su Red Local

Redireccionamiento NAT

Configuración de red NAT

Firewall

Componentes de un firewall distribuido

Microsoft Windows XP. Using Windows Firewall

Filtrado de paquetes en redes con iptables

Redes inalámbricas

Seguridad en redes wi-fi inalámbricas

Microsoft Windows. Configuración de redes inalámbricas IEEE 802.11 de Windows XP para el hogar y la pequeña empresa

Efectuar respaldos de la información

Microsft Windows. Cómo programar backups automáticos

Microsoft Windows. Backup Under the Full Recovery Model

Llevar a cabo un mantenimiento preventivo de los recursos tecnológicos

Mantenimiento preventivo

Mantenimiento de software

Brindar seguridad física a los recursos tecnológicos

Definición de aspectos eléctricos (UPS y Grupo Generador) a ser tomados en cuenta al momento de diseñar un Centro de Datos (CPD)

Consideraciones necesarias para el diseño de un Centro de Proceso de Datos (CPD)

Estándares sobre diseño y funcionamiento para centro de datos

Bibliografía (en anexo)