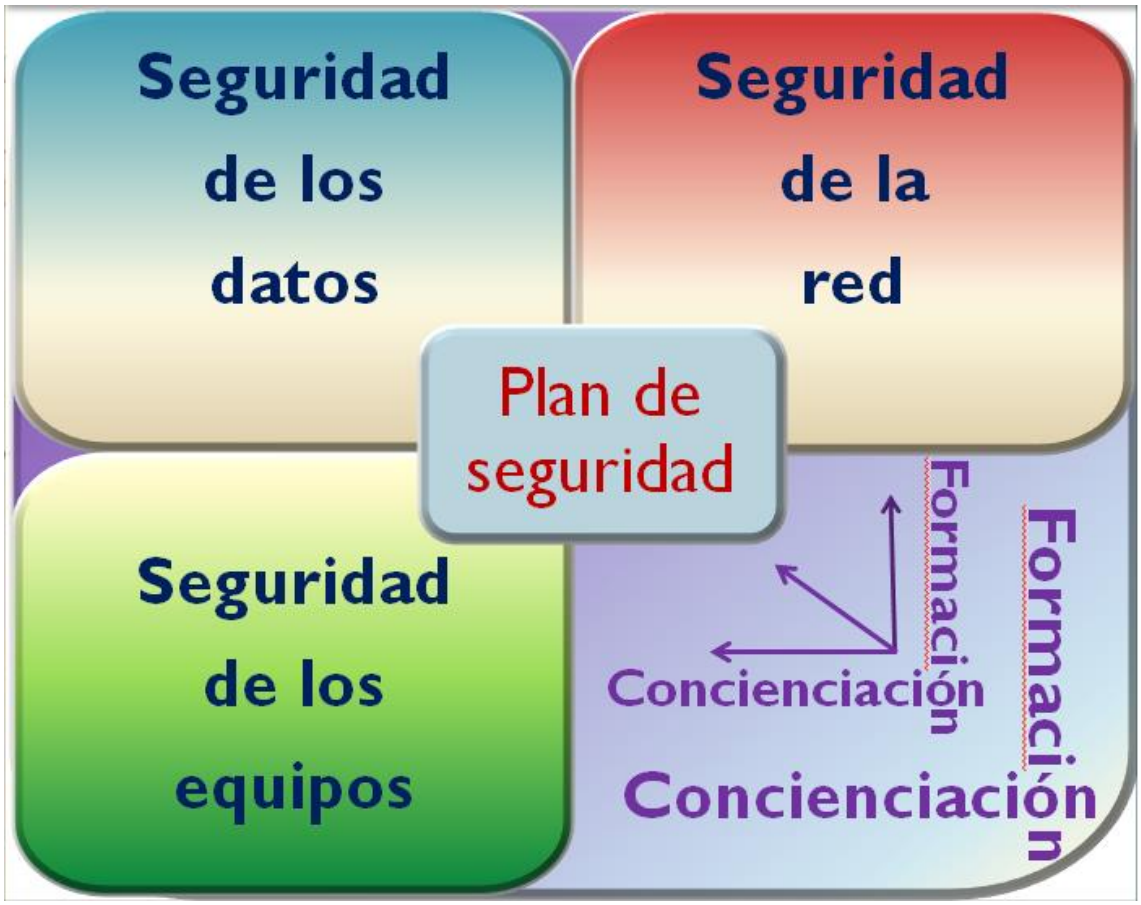
Javier Rubio Villacé
Asesor TIC del Área de Programas Educativos de la Dirección Provincial de Educación de Valladolid



Protección, confidencialidad, conservación y seguridad de los datos de carácter académico y educativo

Criterios que se están cumpliendo en la actualidad (Situación de partida) + los que deberán cumplirse (actuaciones de mejora)

- **Control de acceso a los datos**
  - ***Relación de los ficheros con informaciones sensibles que se usan en el centro***
    - Nombre del archivo
    - Tipo de datos que contiene
    - Ubicación
    - Cifrado. Herramienta utilizada.
  - ***Relación de equipos en los que se encuentran los datos protegidos***
    - Nombre netbios
    - Dirección IP
    - Perfiles de acceso
    - Recursos que comparten en la red
    - Procedimientos de identificación y autenticación
    - Registro de extracción de datos, que documente:
      - Fecha
      - Nombre del archivo de datos.
      - Autor
      - motivo de la extracción
    - Herramienta para control de dispositivos USB.
  - ***Gestión de contraseñas (*)***
    - Procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad e integridad.
      - Persona encargada de la custodia.
      - Contraseñas diferentes para servicios diferentes.
      - Cambiarlas con regularidad.

  - Construirla combinando letras mayúsculas y minúsculas con números, añadiremos otros símbolos (+,-,?,!,...) en caso contrario. Con no menos de 8 caracteres.
  - Utilizar una herramienta de gestión de contraseñas.

- ***Soportes utilizados para el almacenamiento de ficheros***
  - Inventario de soportes.
  - Registro en el que se anotan las entradas y salidas.
  - Lugar de almacenamiento.
  - Mecanismos para que solamente puedan acceder las personas autorizadas:
    - Cifrado de los datos. Herramienta de cifrado de datos.
  - Herramienta para bloquear el uso de pendrives en los equipos de administración.
- ***Copias de seguridad***
  - Equipo responsable.
  - Periodicidad: con qué frecuencia se realizan.
  - Tipo: automática o manual.
  - Registro de copias de seguridad
    - Fecha
    - Autor
    - Ubicación
    - Cifrado.
  - Herramientas utilizadas.
  - Lugar de almacenamiento.
- ***Difusión y extensión de datos personales dentro y fuera del centro***
  - Registro de la redes sociales con acceso autorizado desde el centro.
  - Elaborar estrategias para crear la identidad digital del centro.
  - Elaborar estrategias para formar y concienciar a los alumnos sobre el uso correcto de los datos y la tecnología.
    - Imágenes, difusión de datos personales en Internet, acceso a contenidos inapropiados en la red.

Seguridad de la red

- **Equipo responsable. Tareas a realizar:**
  - Miembros del equipo
  - Establecer criterios de uso, configuración y acceso a los sistemas (usuario, contraseña,…).
    - (*) Gestión de contraseñas.
  - Comprobar si están funcionando las medidas de seguridad previstas.
    - Garantizar que no se interrumpan los servicios.
    - Detectar y solucionar en primera instancia las incidencias de seguridad detectadas.
  - Crear y registrar las directivas de grupo utilizadas para definir las configuraciones de los equipos y usuarios.
    - Evitar que personas no autorizadas accedan el sistema.
    - Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
  - Informar y educar a los usuarios sobre el uso seguro de los sistemas.
  - Definir los posibles riesgos y las medidas a tomar.
  - Llevar a cabo la auditoria de los sistemas.
- **Seguridad inalámbrica**
  - Equipo responsable del funcionamiento y la configuración de los AP.
  - Registro de los puntos de acceso de la LAN. Se incluirá en la documentación de la red con los siguientes datos:
    - Ubicación
    - ESSID
    - Dirección IP de administración.
    - Frecuencia (2,4 o 5 GHz) y canal de funcionamiento.
    - Período de funcionamiento.
    - Tipo de protección:
    - (*) Gestión de contraseñas:
    - Tipo de cifrado
    - Filtrado MAC:
      - Registro de equipos con acceso permitido o denegado.
    - Aislamiento AP

- IP de la subred y configuración del router (si existe).
- Lista de control de acceso (AC) del cortafuegos (si existe).

➢ Controlador de dominio

- Persona responsable.
- Documentar la configuración del servidor y del dominio:
  - Nombre del dominio.
  - Dirección IP.
  - Registro de las directivas de grupo activas.
  - Perfiles de usuario.
  - Unidades de red.
  - Gestión de contraseñas:
    - Período de validez, fortaleza.
  - Antivirus corporativo.

➢ Subredes

- Documentar la seguridad implementada en las subredes en funcionamiento:
  - Medidas de seguridad activas en cada una de ellas.
  - Enrutamiento entre ellas y mapeo de puertos (si existiera).
  - Listado de recursos accesible y bloqueados.
  - Relación de usuarios o grupos con acceso.

➢ Acceso a Internet

- Equipo responsable.
- Establecer criterios de responsabilidad de uso (buenas prácticas).
- Establecer criterios de control de acceso, que permitan identificar incidencias de seguridad o mal uso, identificando riesgos y estableciendo posibles medidas de respuesta:
  - Equipo o persona responsable.
  - Herramienta de control parental
    - Listado de recursos con acceso no autorizado desde la red local a Internet.
    - Registro de sitios web, redes sociales y blog con acceso recomendado.
  - Sistema para la detección de acceso a recursos no permitidos en Internet o descargas de materiales ilegales desde la red del centro:

- Servidor de seguridad con sistema de monitorización y generación de informes de la actividad de los usuarios en Internet (del tipo *Squid+Sarg*)
- Procedimiento para averiguar el usuario que realizó el acceso o descarga ilegal.
- Medidas de respuesta.

- Router ADSL
  - Credenciales de acceso como administrador.

    Protocolo de acceso (generalmente http), dirección IP, nombre de usuario y contraseña (gestión de contraseñas)
  - Documentar puertos abiertos (mapeo de puertos).
- Documentar servidor de seguridad:
  - Sistema operativo.
  - Cortafuegos: *Iptables, SonicWALL,...*
  - Reglas de salida a Internet y acceso a la red local.

Seguridad de los equipos

- **Equipo responsable. Tareas:**
  - Comprobar que las herramientas de seguridad funcionan y se actualizan correctamente.
  - Escanear los equipos con antivirus y antimalware con la periodicidad que se considere conveniente.
  - Detectar incidencias y aplicar medidas en respuesta a ellas.
  - Fijar criterios de acceso y configuración:
    - Usuario, contraseña, perfiles.
  - Fijar criterios de responsabilidad de uso (buenas prácticas).
- **Registro de aplicaciones de seguridad instaladas**
  - Antivirus
  - Antimalware
  - Control parental
  - Cortafuegos
  - Congeladores de disco
- **Programas de gestión académica**

  Regulado mediante Instrucción de 27 de mayo de 2013, de la Dirección General de Política Educativa Escolar.

Formación y concienciación

- **Estrategias para formar y concienciar a los alumnos en el uso correcto y seguro de las nuevas tecnologías.**
  - Tutorías.
    - Temas:
      - Suplantación de identidad
      - Redes Sociales, Whatsapp,…
      - Ingeniería Social.
      - Uso de Dispositivos Móviles.
      - Riesgos en Internet: *Ciberbullying, Grooming, Sexting*
      - *Identidad digital.*
      - *…*
  - Talleres.
- **¿El Reglamento de Régimen Interior recoge los procesos y actuaciones a aplicar en el caso de uso inadecuado e incidencias en materiales y servicios?**

  Se deben establecer unas pautas de uso de los equipos informáticos por parte de cualquier miembro de la comunidad educativa, especialmente por el profesorado y alumnado.