



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 10

1. Seguridad física de un sistema de información.
2. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento.
3. Auditoría de seguridad física.



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 10

Seguridad física de un sistema de información. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento. Auditoría de seguridad física.

1. SEGURIDAD FÍSICA DE UN SISTEMA DE INFORMACIÓN.

La seguridad física proporciona protección ante accesos no autorizados, daños e interferencias a las instalaciones de la organización y a la información. Los requisitos sobre seguridad física varían considerablemente según las organizaciones y dependen de la escala y de la organización de los sistemas de información. Pero son aplicables a nivel general los conceptos de asegurar la protección de ciertas áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad.

Desde el punto de vista legal hay que tener en cuenta:

En relación con aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Adoptar las medidas técnicas y de organización, necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.

En relación con la protección de los datos de carácter personal (Real Decreto 994/1999):

- Autorizar la ejecución del tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero, por el responsable del fichero.
- Autorizar el acceso físico de forma exclusiva al personal autorizado en el documento de seguridad.

Los criterios para realizar estas tareas son:

- Se debe situar el equipamiento que soporta a la aplicación, así como los soportes de información, en áreas seguras y protegidas adecuadamente.

- Se deben definir de forma proporcionada las medidas que garanticen la seguridad de los locales a proteger en relación con los requisitos de seguridad de la información que se almacene o procese.
- Se deben construir barreras físicas del suelo al techo para prevenir entradas no autorizadas o contaminación del entorno. Las ventanas y puertas de las áreas seguras deben estar cerradas y controlarse periódicamente. Las ventanas deben protegerse externamente. Se pueden necesitar barreras adicionales y perimetrales entre áreas con diferentes requisitos de seguridad dentro del perímetro global de seguridad.
- Se deben construir las instalaciones de forma discreta y minimizar las indicaciones sobre su propósito, evitando signos obvios (fuera o dentro del edificio) que identifiquen la presencia de las actividades cuya seguridad se desea. No informar al personal que no esté directamente implicado de las actividades que se hacen dentro de las áreas seguras.
- No se deben identificar en directorios telefónicos y de los vestíbulos de la organización las localizaciones informáticas (excepto las oficinas y áreas de recepción).

2. RIESGOS, AMENAZAS Y VULNERABILIDADES. MEDIDAS DE PROTECCIÓN Y ASEGURAMIENTO.

Se deben proteger los locales de amenazas potenciales:

- Eléctricas: realización de un proyecto eléctrico para la instalación, que asegure la independencia de las líneas eléctricas de los equipos de las líneas de fuerza (motores, alumbrado, etc.) del edificio, la seguridad de las personas y de los equipos mediante un adecuado diseño de los cuadros eléctricos y de las protecciones diferenciales magnetotérmicas y filtros, la disponibilidad mediante sistemas de alimentación ininterrumpida, equipos electrógenos, etc., el correcto estado del sistema de puesta a tierra del edificio, una correcta instalación de la malla de tomas a tierra en el falso suelo, una correcta canalización y protección de los cables, etc. La instalación de un suelo técnico adecuado, en sus características antiestáticas y conductoras, a los equipos y los riesgos de las labores que se realizan en la sala. La instalación de sistemas de alarmas efectivos ante contingencias.
- Incendios: cumplimiento de las normas relativas a protección de incendios, vigilando la señalización, prohibiciones de fumar, no acumulación de papel y la no ocupación de las vías de salida de emergencia. Instalación de sistemas de detección, alarma y extinción de incendios, y su revisión periódica. Disponibilidad de armarios ignífugos para el almacenamiento de las copias de respaldo.
- Clima: instalar sistemas de control de la temperatura y de la humedad.
- Agua: instalar sistemas de detección y evacuación de agua. Elegir ubicación sin canalizaciones cercanas de agua.
- Interferencias: evitar interferencias electromagnéticas, como las provenientes de los dispositivos móviles, cebadores de los fluorescentes, etc.
- Agentes químicos: considerar el uso de protecciones especiales para equipamientos situados en ambientes particularmente agresivos.
- Otros: elegir la ubicación evitando excesivas vibraciones. Control del polvo mediante limpieza regular y pinturas especiales para el suelo de la sala que evite su acumulación.

- Se deben documentar debidamente los procedimientos de emergencia y revisar esta documentación de forma regular.
- Se deben formar al personal en el funcionamiento de todos los sistemas instalados, realizando simulaciones de contingencias.
- Se deben implantar medidas para proteger los cables de líneas de datos contra escuchas no autorizadas, contra daños (por ejemplo, evitando rutas a través de áreas públicas o fácilmente accesibles), o interferencias (por ejemplo, evitando recorridos paralelos y cercanos a líneas eléctricas). Instalar las líneas de suministro y telecomunicaciones para servicios de los sistemas de información en instalaciones comunes, subterráneas cuando sea posible, o tener medidas alternativas de protección adecuada.
- Se deben ubicar los terminales que manejen información y datos sensibles en lugares donde se reduzca el riesgo de que aquéllos estén a la vista.
- Se deben almacenar los materiales peligrosos y/o combustibles a una distancia de seguridad del emplazamiento de los ordenadores. Por ejemplo, los suministros informáticos como el papel no se deben almacenar en la sala de ordenadores (hasta que se necesiten). Inspeccionar el material entrante, para evitar amenazas potenciales, antes de llevarlo al punto de uso o almacenamiento.
- Se deben ubicar el equipamiento alternativo y copias de respaldo en sitios diferentes y a una distancia conveniente de seguridad. Estas copias de respaldo se almacenarán en armarios ignífugos.
- Se deben controlar la entrada en exclusiva al personal autorizado a las áreas que se hayan definido como áreas a ser protegidas. Autorizar sólo con propósitos específicos y controlados los accesos a estas áreas, registrando los datos y tiempos de entrada y salida.
- Obligar a todo el personal a que lleve una identificación visible dentro del área segura y que observe e informe de la presencia de personal extraño al área. En éstas se deben prohibir los trabajos no autorizados en solitario para evitar la oportunidad de acción maliciosa. Cerrar la puerta externa del área, cuando la interna esté abierta.
- Se debe restringir el acceso a las áreas seguras del personal de los proveedores o de mantenimiento a los casos en que sea requerido y autorizado. Aun con acceso autorizado deben restringirse sus accesos y controlarse sus actividades (especialmente en zonas de datos sensibles).
- Se deben definir normas y controles relativos a la posible salida/entrada física de soportes de información (impresos, cintas y disquetes, CDs, etc.), así como de los responsables de cada operación.

Es básico tener en cuenta las siguientes recomendaciones:

En relación con la adecuación de locales:

- Separar las áreas de carga y descarga de material de las áreas a proteger. En caso de que esto no sea posible, se deberán establecer los controles adecuados para impedir accesos no autorizados.
- Restringir los accesos al área de carga y descarga, desde fuera del edificio, al personal autorizado y debidamente identificado.

En relación con la instalación de líneas de telecomunicaciones:

Considerar medidas adicionales para sistemas sensibles o críticos, como:

- Instalación de conductos blindados, salas cerradas, etc.
- Uso de rutas o medios de transmisión alternativos.

En relación con la ubicación de equipamiento, materiales y copias de respaldo:

- Situar en áreas seguras los equipos a proteger donde se minimicen los accesos innecesarios a las áreas de trabajo, distanciadas de las zonas de acceso público y de las zonas con aproximación directa de vehículos públicos. Definir perímetros de seguridad con las correspondientes barreras y controles de entrada. Su protección física debe impedir accesos no autorizados, daños y cualquier otro tipo de interferencias.

La protección de los soportes de información (discos duros, disquetes, CD-ROM, cintas, ordenadores portátiles, etc.) debe incluir un conjunto equilibrado de medidas proporcionado a la naturaleza de los datos y documentos que contengan.

En la preparación de los procedimientos de protección de los soportes de información ha de tenerse en cuenta que los ordenadores personales, incluyendo los portátiles, agendas electrónicas, etc., con discos fijos u otros dispositivos de almacenamiento no volátiles, operando de forma aislada o conectados en red, deben ser considerados como dispositivos de almacenamiento de información en el mismo sentido que otros soportes electrónicos de almacenamiento de información extraíbles.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Los documentos que contengan actos administrativos que afecten a derechos o intereses de los particulares podrán conservarse en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo.
- Deberán existir medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados.

En relación con la protección de datos de carácter personal (Real Decreto 994/1999):

Datos de carácter personal a los que se ha de aplicar medidas de seguridad de nivel básico:

- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.
- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

- El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.
- Establecer procedimientos para la realización de copias de respaldo y para la recuperación de datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- Realizar copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Datos de carácter personal para aplicar medidas de seguridad de nivel medio (Real Decreto 994/1999):

- Disponer de un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
- Disponer de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.
- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel alto (Real Decreto 994/1999):

- La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.
- Conservar una copia de respaldo y los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas exigidas en este reglamento.

Habrà que tener en cuenta los siguientes criterios:

1. Se debe aplicar lo previsto en el documento «Criterios de Conservación» en los apartados de «Seguridad de la información» y «Protección frente al deterioro físico» desarrollar y aplicar procedimientos de seguridad que contemplen la autenticidad, confidencialidad, integridad y disponibilidad, el tratamiento de datos de carácter personal, la gestión de soportes removibles, la eliminación y destrucción de soportes y la documentación del sistema de conservación.

2. Se deben establecer procedimientos de realización, recuperación y pruebas de las copias de respaldo que contemplen copias de los programas, aplicaciones, documentación, bases de datos, sistemas operativos, logs, etc.; debe definirse la periodicidad con que se realizan las copias (diaria, semanal, mensual), número de copias que se realizan y versiones distintas que se conservan. Los procedimientos de realización de copias serán automáticos y periódicos.
3. Se debe elegir un lugar de almacenamiento adecuado para los soportes de información. Se debe tener en cuenta lo previsto en el capítulo «Seguridad física».
4. Para ficheros a los que haya que aplicar medidas de nivel alto se debe recurrir a dos copias distintas una de las cuales debe guardarse en una ubicación diferente de donde se encuentren los equipos informáticos que las tratan.
5. Se debe mantener un registro de entrada y salida de los soportes de información. Permitirá conocer: el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. Cabe recoger asimismo el número de serie del soporte y marca de clasificación.
6. Los soportes de información enviados o distribuidos al exterior que contengan datos de nivel alto deberán ser cifrados.
7. Verificar la definición y correcta aplicación de las medidas de protección de los soportes de información.
8. Se debe incluir entre las prácticas de protección de los soportes de información medidas básicas como las siguientes, dentro y fuera del horario normal de trabajo, para evitar su pérdida o destrucción:
 - Los documentos, disquetes y otros soportes de información deben guardarse en armarios cuando no se usen y, especialmente, fuera del horario normal de trabajo.
 - La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o la oficina esté vacía.
 - Los ordenadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.
9. Se debe verificar que los usuarios cumplen las recomendaciones relativas a que los equipos no atendidos queden convenientemente protegidos.
10. Realizar periódicamente pruebas para verificar que la recuperación de la información a partir de las copias de respaldo funciona correctamente. Estas pruebas se pueden basar en inspecciones periódicas de forma aleatoria o exhaustiva para comprobar su presencia física y contenido.

Se deben tener en cuenta las siguientes recomendaciones:

- Proteger la entrada y salida de correo, así como los puntos de fax desatendidos.
- Considerar que la denominación del nivel de seguridad aplicable aparezca señalada de forma inequívoca en todos sus soportes.

- Reflejar el nivel de seguridad aplicable en todas y cada una de las páginas de los impresos, incluyendo la carátula; opcionalmente el nivel de seguridad puede figurar en la cabecera o en el pie de página, siempre que resulte fácilmente legible.
- Reflejar el nivel de seguridad aplicable en todas y cada una de las pantallas que aparezcan en los terminales o puestos del usuario, o estar permanentemente en la cabecera de la pantalla.
- Etiquetar cada soporte electrónico transportable (cintas, cartuchos, disquetes, etc.) con el máximo nivel de seguridad de la información que contenga.
- Si la información (por ejemplo, datos de carácter personal a los que se han de aplicar medidas de nivel medio o alto) se envía al exterior o por correo externo a la organización, el sobre cerrado y marcado con el citado nivel de seguridad deberá introducirse en un contenedor NO marcado.
- Incluir en las copias de respaldo los ficheros de registros de eventos (trazas de audit, logs) y diario de incidencias.
- Emplear en las copias de respaldo formatos no propietarios que garanticen su accesibilidad en el tiempo.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.

En relación con la protección de los datos de carácter personal (Real Decreto 994/1999).

- Garantizar los niveles de seguridad que les corresponda a los ficheros temporales con arreglo a los criterios establecidos.
- Borrar todo fichero temporal una vez haya dejado de ser necesario para los fines por los que fue creado.
- Identificar, inventariar y almacenar en lugar con acceso restringido cualquier soporte informático con información que contenga datos de carácter personal.
- Autorizar, por parte del responsable, la salida fuera de los locales en los que esté ubicado el fichero, de cualquier soporte informático con información que contiene datos de carácter personal.
- Realizar pruebas anteriores a la implantación o modificación de aplicaciones con datos no reales.

Habrà que tener en cuenta los siguientes criterios:

1. Se deben adoptar procedimientos de explotación adecuados para salvaguardar la disponibilidad, integridad y confidencialidad de la información.
2. Se deben definir procedimientos para el paso de aplicaciones a explotación, ya sean nuevas o actualizaciones de las existentes, que recojan los requisitos que éstas deben cumplir y las pruebas a realizar antes de su aceptación.

3. Se debe asegurar, por medio de la gestión de configuración y de cambios, que las modificaciones en el sistema no reducen la efectividad de las salvaguardas ni la seguridad general del mismo, que se identifican nuevos requisitos de seguridad o impacto en la seguridad de los posibles cambios y que los mismos tienen reflejo en el plan de contingencias.
4. Se deben realizar mantenimientos preventivos, como la instalación de las actualizaciones de seguridad recomendadas por los fabricantes, o el aumento de capacidad para evitar saturaciones.
5. Se debe documentar en la política de seguridad los requisitos con relación a licencias de programas y la prohibición de uso e instalación de software no autorizado. Establecer controles periódicos que revisen el software instalado e implantar mecanismos de protección para evitar la instalación de software no autorizado.
6. Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.
7. Se debe aplicar el análisis y gestión de riesgos para determinar las necesidades de seguridad de la aplicación antes de su desarrollo e incorporar las funciones de salvaguarda antes de completarla (más barato y efectivo).
8. Se deben tener en cuenta los aspectos de seguridad de la aplicación en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y el mantenimiento e incorporando las funciones de salvaguarda antes de su puesta en explotación.

Se deben tener en cuenta las siguientes recomendaciones:

En relación con el desarrollo:

- Establecer criterios de aceptación para nuevos sistemas, así como en los desarrollos de nuevas versiones y funciones.
- Para la realización de las pruebas previas a la puesta en explotación (relativas a la seguridad, rendimientos, diseño, etc.) es conveniente la disposición de un entorno de pruebas independiente de los entornos de desarrollo y de explotación.
- En condiciones de determinados requisitos de seguridad cabe desarrollar un Perfil de Protección conforme con los Criterios Comunes de evaluación de la seguridad de las tecnologías de la información.

En relación con la explotación:

- Implantar y mantener actualizado el software de detección y protección ante código dañino y de detección de intrusiones.
- Formar a los usuarios en la utilización adecuada de la aplicación, del software antivirus y en la notificación de incidencias relacionadas con los ataques de este tipo y todo lo relativo a la gestión y responsabilidades relacionadas con el código dañino.

Gestión y registro de incidencias.

Se trata de una función esencial para el análisis de los problemas informáticos y en especial de los incidentes de seguridad. Se entiende la «informática forense» como aquella que se ocupa de investigar los incidentes o intrusiones, una vez que éstos ya se han producido, para tratar de averiguar las causas, los autores y los daños que han conllevado.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.
- Las medidas de seguridad deberán garantizar la prevención de alteraciones o pérdidas de los datos e informaciones y la protección de los procesos informáticos frente a manipulaciones no autorizadas.

En relación con la protección de los datos de carácter personal (Real Decreto 994/1999):

Datos de carácter personal a los que se han de aplicar las medidas denominadas de nivel básico:

- Notificar y gestionar las incidencias utilizando un registro en el que conste el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién lo comunica y los efectos que se hubieran derivado de la misma.

Datos de carácter personal a los que se han de aplicar las medidas denominadas de nivel medio y alto:

- Consignar además de los datos mencionados en el punto anterior, los procedimientos realizados para recuperar los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorizar por escrito del responsable del fichero para ejecutar los procedimientos para recuperar los datos.

Habrà que tener en cuenta los siguientes criterios:

1. Se debe definir el procedimiento de gestión de incidencias, que establezca las formas de comunicación, el diagrama de estados por los que pasará hasta su conclusión, la clasificación según su gravedad, las condiciones para el escalado de la incidencia a los responsables de la organización, la forma de comunicación a proveedores externos, consulta del estado de las incidencias, etc.
2. Se debe formar y concienciar a los usuarios en relación con los procedimientos de comunicación, consulta y reacción ante incidencias. Se deben establecer canales para informar lo más rápidamente posible de las incidencias y el mal funcionamiento de los sistemas.

3. Se debe implantar un registro de incidencias acorde al procedimiento y a los datos manejados con el tipo de incidencia, momento, persona que realiza la notificación, a quién lo notifica y los efectos de la misma. Esta información junto con otra relativa a la seguridad se debe conservar para aprender de estas experiencias, con objeto de minimizar los posibles daños y consecuencias, para investigaciones futuras y para el control de los accesos.
4. Si sospecha que el mal funcionamiento es debido a problemas de software (por ejemplo, un virus), el usuario debe:
 - Observar los síntomas y mensajes que aparezcan en pantalla.
 - Dejar de usar el sistema (aislarlo si es posible, pero no apagarlo) e informar de inmediato a la unidad de soporte informático.
 - Informar inmediatamente a su mando responsable por el canal determinado.
 - La organización informará a los usuarios que ellos no deben, en ninguna circunstancia, intentar retirar el software sospechoso. Esto debe realizarse por un experto debidamente entrenado y con experiencia. Si el experto va a realizar las pruebas en la máquina del usuario, ésta se desconectará de las redes de la organización antes de volver a arrancarla.

Se deben tener en cuenta las siguientes recomendaciones:

- Los actores implicados conocerán los procedimientos para realizar y remitir informes sobre los diferentes tipos de incidencias, las amenazas, vulnerabilidades o simplemente el mal funcionamiento de la aplicación o del sistema, a quién deben ir dirigidos, así como la respuesta con las acciones a ejecutar.
- Controlar y cuantificar los distintos tipos de incidentes, causa u origen e impacto causado.
- La organización debe pedir a los usuarios que observen e informen sobre toda aplicación o programa que parezca que no está funcionando bien (es decir, de acuerdo con las especificaciones).
- Es conveniente el desarrollo de planes de informática forense, y la implantación de herramientas para su ejecución, que permitan aclarar incidencias ocurridas.

3. AUDITORÍA DE SEGURIDAD FÍSICA.

Definición de auditoría: proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que se compara la evidencia (ISO 9000: 2000).

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Adoptar medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad y disponibilidad, garantizando la restricción de utilización, la prevención de alteraciones y la protección a procesos informáticos.

En relación con la protección de los datos de carácter personal a los que se ha de aplicar las medidas de nivel medio y alto (Real Decreto 994/1999):

- Someter a una auditoría interna o externa a los sistemas de información e instalaciones de tratamiento de datos, esta auditoría verificará el cumplimiento del Reglamento del Real Decreto 994/1999.
- Emitir un informe de auditoría que deberá dictaminar sobre la adecuación de las medidas y controles del mencionado reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Analizar los informes de auditoría por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Habrá que tener en cuenta los siguientes criterios:

1. La situación y actividades de seguridad se deben revisar de forma independiente (auditoría) y periódicamente para asegurar que las prácticas de la organización siguen estas normas y que además son efectivas.
2. En relación con la protección de datos de carácter personal a los que haya que aplicar las denominadas medidas de nivel medio o alto, se deben someter a auditoría los sistemas de información e instalaciones de tratamiento de datos al menos cada dos años.
3. La aplicación debe estar dotada de un registro de eventos o pista de auditoría que registre al menos el identificador de usuario, fecha, hora, y proceso mediante el que se ha realizado un alta, modificación o baja de cualquier información que substancie el ejercicio de una potestad, afecte a datos de carácter personal o pueda ser considerada como sensible.
4. Se deben proteger los ficheros de recogida de eventos así como las herramientas de auditoría y control, a fin de evitar su alteración o destrucción por medios no autorizados para salvaguardar su integridad y su disponibilidad, especialmente los del registro telemático y el servicio de dirección electrónica única.
5. Se deben sincronizar los relojes de los distintos sistemas para facilitar un archivo fiable de eventos.
6. Se debe controlar periódicamente la utilización de los distintos componentes del sistema.
7. Se debe asegurar que la función de auditoría accede en su caso a la información relativa a las medidas de seguridad, pero no a los datos.
8. En las aplicaciones que se citan a continuación, el registro de eventos guardará al menos traza:
 - En el servicio de dirección electrónica única, se guardará traza de la fecha y la hora del acceso del interesado al contenido de la notificación y traza de la fecha y hora de remisión del aviso de notificación al interesado.
 - En el registro telemático se guardará traza de la fecha y hora de recepción en el registro de la solicitud, escrito o comunicación.

Se deben tener en cuenta las siguientes recomendaciones:

- Revisar periódicamente que los usuarios cumplen con los requisitos de seguridad que les son aplicables (por ejemplo, actualización de contraseñas, conservación de la información en el puesto de trabajo, etc.).
- Revisar periódicamente las medidas organizativas y técnicas de seguridad para mejorarlas y aumentar su eficacia.
- Realizar periódicamente los denominados análisis de vulnerabilidades, con ayuda de herramientas disponibles en el mercado, para detectar y poder corregir los posibles agujeros de seguridad en los sistemas.

