COMO AUDITAR EL CUMPLIMIENTO DE LA LORTAD /LOPD / REGLAMENTO DE SEGURIDAD

Rafael Bernal, CISA

Universidad Politécnica de Valencia

El Reglamento de medidas de seguridad exige para los ficheros de **nivel medio**, en su artículo 17, la obligatoriedad de una auditoría.

Por referirse a los ficheros de nivel medio abarca también los de nivel alto.

Para los sistemas de información que se encontraran en funcionamiento a la entrada en vigor del Reglamento, es decir el día 26 de junio de 1999, las medidas de seguridad de nivel medio (la auditoría entre ellas) deberían estar implantadas en el plazo de un año, es decir hasta el 26 de junio de 2000.

El artículo que se refiere a la Auditoría dentro del Reglamento es el 17, que establece:

1. *Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.*

2. *El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente 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.*

3. *Los informes de auditoría serán analizados 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.*

Respecto al punto 1, es clara la periodicidad: máximo cada dos años.

El **objeto** de la auditoría será verificar el cumplimiento del Reglamento, que variará si los ficheros son de nivel medio o alto, pero que al menos, en nuestra opinión, debe abarcar:

- Ficheros y niveles asignados.

- Acceso a datos a través de redes de comunicaciones: cómo se efectúan y seguridad.

- Régimen de trabajo fuera de los locales de ubicación del fichero: autorización por el responsable del fichero y nivel de seguridad existente.

- Ficheros temporales: que cumplan el nivel de seguridad (las protecciones que les correspondan), así como que son borrados una vez que han dejado de ser necesarios para los fines que motivaron su creación.

- Documento de seguridad: existencia, idoneidad según el Reglamento y cumplimiento. Se verificará además que está actualizado, así como que se ha revisado si se han producido cambios relevantes en el sistema de información o en la organización del mismo.

  También es necesario comprobar que el contenido del documento se ha adecuado a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

  (La revisión del "Documento de Seguridad" y de su cumplimiento puede ser uno de los puntos más laboriosos).

- Las "Funciones y Obligaciones del personal": de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información.

  Se verificará si están claramente definidas y documentadas, y en la auditoría debería contrastarse si en la realidad se cumplen. También es necesario verificar que el responsable del fichero ha adoptado las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- El "Registro de Incidencias" : además del "procedimiento de notificación, gestión y respuesta ante las incidencias" dentro del Documento de Seguridad, la existencia e idoneidad del propio registro y si su contenido cumple el contenido del artículo 10. En el Reglamento no se indica si el registro ha de ser en papel o electrónico, por lo que cualquier modalidad puede ser en principio válida.

  En la práctica este registro podría ser compartido con otros tipos de incidencias, no sólo las que afectaran a datos de carácter personal, siempre y cuando se cumplan los puntos que exige el Reglamento.

- La identificación y autenticación ante los sistemas: existencia de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información, y si se han establecido procedimientos de identificación y autenticación para dicho acceso.

  En entidades grandes una relación nominal difícilmente podría mantenerse bien actualizada, debido a los cambios constantes, por lo que tal vez podría valer una relación de funciones, y algún sistema por el que se sepa qué personas tienen asignadas las funciones en cada momento, si bien este

punto no lo detalla así el Reglamento, por lo que hay que ser cautos en las interpretaciones que hacemos en la práctica.

Si la autenticación se basa en contraseñas, existencia, idoneidad y cumplimiento de un procedimiento de asignación, distribución y almacenamiento, que garantice su confidencialidad e integridad.

Asimismo, se deberá verificar si las contraseñas se cambian con la periodicidad que se determine en el documento de seguridad, y comprobar que mientras estén vigentes se almacenan de forma ininteligible (por ejemplo, cifradas).

- El control de acceso a los datos y recursos: si son los autorizados por el responsable del fichero y según los accesos autorizados para cada usuario según la relación actualizada que deberá existir.

  Asimismo, si la concesión, alteración o anulación de los accesos autorizados sobre los datos y recursos, se llevan a cabo exclusivamente por el personal autorizado en el "documento de seguridad", y según los criterios establecidos por el responsable del fichero.

- Respecto a los soportes informáticos que contengan datos de carácter personal: si permiten identificar el tipo de información que contienen, si están inventariados, si están almacenados en un lugar con acceso restringido al personal autorizado para ello en el "documento de seguridad".

  Asimismo, si la salida de bs soportes fuera de los locales en que esté ubicado el fichero sólo es autorizada por el responsable del fichero.

- En cuanto a las copias de respaldo, se comprobará que el responsable del fichero se encarga de verificar la definición y correcta aplicación de los procedimientos de realización de dichas copias de respaldo, así como en cuanto a la recuperación de los datos. Esto último puede abarcar desde la simple recuperación de un fichero en el caso de que haya resultado dañado, hasta el denominado Plan de Contingencia, si existe.

  Es necesario verificar que dichos procedimientos para la realización de copias de respaldo y para la recuperación de los datos garantizan su reconstrucción "en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción" (esto será difícil de cumplir en la práctica en algunos casos si lo entendemos literalmente).

  También, y sobre todo, que se realizan las copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. (En la práctica la frecuencia mínima vendría dada por la volatilidad de los datos y las dificultades de reconstrucción: en algunos casos las copias deberían ser diarias para garantizar la recuperación, existiendo con frecuencia discos "espejo").

Hasta aquí se han recogido los puntos que deben cumplir los ficheros de **nivel básico**, que no están sujetos a auditoría, pero que deben cumplir también los ficheros de nivel medio, que sí están sujetos a auditoría.

Los puntos que deben cumplir los ficheros de **nivel medio**, y que deben evaluarse en la auditoría, son:

- El contenido del ”documento de seguridad”, que además de lo referido al nivel básico, ha de contener: la identificación del responsable o responsables de seguridad (en la auditoría se debería verificar si se trata de persona/s adecuada/s y del cumplimiento de su responsabilidad), así como la realización de controles periódicos para verificar el cumplimiento de lo dispuesto en el propio documento y de las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

  En este caso caben desde desmagnetizadores, en el caso de que los soportes sean magnéticos, hasta la grabación de varias pasadas con un contenido aleatorio para que no sea legible el contenido anterior.

- También si el responsable o responsables de seguridad han sido designados por el responsable del fichero, y si se encargan de coordinar y controlar las medidas definidas en el “documento de seguridad”.

- Existencia e idoneidad de un mecanismo, establecido por el responsable del fichero, que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, así como la verificación de que está autorizado, y que se limita la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Para esto, en algunos sistemas, puede ser suficiente con limitar, por ejemplo a tres, el número de intentos que se admiten a un usuario.

- También se verificará, en cuanto a accesos físicos, que sólo el personal autorizado en el “documento de seguridad” podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

- En cuanto a los soportes, si existe un sistema de registro de entrada de soportes informáticos que permita conocer, directa o indirectamente, 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.

  También se deberá verificar si existe 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.

Asimismo, si los soportes que vayan a ser desechados o reutilizados están sometidos a medidas para impedir cualquier recuperación posterior de la información almacenada en ellos, previamente a que se proceda a su baja en el inventario.

También si en el caso de que los soportes salgan fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, están previstas y se adoptan las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

- Respecto al "registro de incidencias" ya mencionado, se verificará que además de lo indicado, se consignan las ejecuciones de los procedimientos realizados de recuperación de 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 caso de recuperación, y si es necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

  Tal vez en la práctica ha de existir un mecanismo seguro pero ágil si se necesita la autorización por escrito para la ejecución de los procedimientos de recuperación, lo que en casos extremos podría bloquear la recuperación.

- En cuanto a las pruebas: que no se realizan con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado. Desde hace varios años, hemos sugerido la posible "mimetización" de los ficheros (disociación dice la nueva Ley de Protección de Datos): transformaciones no reversibles que impidan la identificación de individuos concretos, lo que posiblemente pueda constituir una medida válida.

Hasta aquí las verificaciones relativas a los ficheros de nivel medio; en el caso de ficheros de **nivel alto**, además, se verificará lo siguiente:

- Que la distribución de soportes que contengan datos de carácter personal se realiza cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

- Que el registro de accesos es adecuado, guardándose por cada acceso, como mínimo: la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado; la información que permita identificar el registro accedido, cuando el acceso ha sido autorizado.

  También se verificará que los mecanismos que permiten el registro de los datos indicados antes están bajo el control directo del responsable de seguridad competente, y que en ningún caso se permite la desactivación de los mismos.

Asimismo, que los datos registrados se conservan al menos dos años.

Y también que el responsable de seguridad competente se encarga de revisar periódicamente la información de control registrada, y que elabora al menos una vez al mes un informe de las revisiones realizadas y los problemas detectados.

- Respecto a las copias de respaldo y la recuperación, ya mencionadas, en el caso de nivel alto se verificará que se conserva una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan, y que se cumplen las medidas de seguridad indicadas en el Reglamento.

  En la práctica no nos solemos conformar con que estén en un edificio diferente, o en otra planta del mismo edificio, si las amenazas son similares, siendo recomendable una distancia mínima: algunas entidades tienen las copias en una ciudad diferente.

- También se verificará que la transmisión de datos de carácter personal a través de redes de telecomunicaciones se realiza cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CONCLUSIONES

Hasta aquí se han indicado los puntos a revisar en la auditoría, que puede ser interna o externa, y no se indica que tenga que ser una “auditoría informática” o “auditoría de sistemas de información” (al parecer, así se sugirió en su día a la Agencia de Protección de Datos cuando se pidió opinión sobre un borrador de Reglamento).

Lo que parece claro es que quienes realicen la auditoría han de ser independientes y objetivos, y estar suficientemente preparados, lo que en el caso de algunos puntos exige una preparación técnica suficiente. La posesión del Certificado de Auditor CISA, y la metodología COBIT creemos que es una garantía suficiente de conocimientos, experiencia y profesionalidad para realizar este tipo de Auditoria.

La propia APD tiene varios CISA’s entre su personal técnico, así como la Agencia Tributaria, el Banco de España, el Ministerio de Administraciones Públicas, .. y esto sin duda creemos que contribuirá a que se vaya normalizando la metodología, técnicas y responsabilidad exigibles a una Auditoria tan exigente y delicada como la de protección de Datos.