UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE INFORMÁTICA

GRADO DE INGENIERÍA INFORMÁTICA
AUDITORÍA INFORMÁTICA

Un auditor ha auditado el cumplimiento de las medidas de seguridad del RDLOPD en veinte ficheros numerados del 1 al 20 con DCP de distintos niveles cada uno de ellos.

Para cada uno de los 20 ficheros auditados indicar según le evidencia constatada:

1. El artículo y apartado del mismo que aplica a la evidencia.
2. El nivel de la medida de seguridad correspondiente a ese artículo.
3. Si se cumple el artículo según el nivel de los DCP el fichero.
4. En caso de no cumplimiento, recomendación del auditor. Si el auditor lo considera, puede realizar recomendaciones aunque se cumpla la medida de seguridad.

Num.	Nivel DCP	Evidencia	Artículo Punto	Nivel Medida	Cumple Artículo	Recomendación del auditor
1	Medio	En el DS no se ha podido constatar la definición de funciones y obligaciones del personal	88.3.B	B	N	Se incluya
2	Alto	El DS no incluye los procedimientos de copias de respaldo y de recuperación	102	A	N	Se debe de incluir
3	Básico	Una copia de las salvaguardias semanales se almacenan en el centro de una empresa de servicios. En el DS no se incluyen referencias.	88.5	B	N	Debe haber una referencia expresa al contrato o documento que regule las condiciones del encargo a una tercera parte
4	Medio	El personal entrevistado desconoce las normas de seguridad	89.2	B	N	El personal debe ser concienciado al respecto, así como las consecuencias en caso de incumplimiento.
5	Alto	En una entrevista con usuarios se ha constatado que algunos tienen acceso a dcp y funciones de las aplicaciones que nunca han usado	89.1 91.X	B	N	-Las funciones y obligaciones de cada usuario con acceso a los dcps deben estar claramente definidos. -Los usuarios solo deben tener acceso solo a aquellos fichero que necesiten para su trabajo. También debe haber un mecanismo que evite el acceso a datos que no necesitan.
6	Básico	No se dispone de un inventario de soportes que contengan dcp	92	B	N	Los soportes deben ser identificable por tipos, y ser inventariados.

7	Medio	En una visita de inspección garaje del edificio se ha constatado la existencia de cajas con documentos en soporte papel que contienen dcp	83	B	N	El responsable de ficheros o tratamiento debe adoptar medidas para limitar el acceso a dcp, o a los soportes que lo contengan. Esa caja de documentos debe estar guardado en un lugar seguro(por ejem: sala de archivos).
8	Alto	Se ha constatado que los usuarios de un departamento comparten la misma contraseña	93.3	B	N	La contraseña debe ser asignados, distribuido, y almacenados mediante un procedimiento que garantice si confidencialidad(por lo que no puede haber 2 iguales) e integridad.

9	Básico	El sistema obliga a cambiar las contraseñas de los usuarios administradores cada 12 meses	93.4	B	N	El Real Decreto explicita “las contraseñas”, por lo que se entiende que todas las contraseñas deben ser cambiadas como máximo anualmente.
10	Medio	El RF no verifica cada seis meses el correcto funcionamiento de los procedimientos de salva y recuperación	94.3	B	N	El responsable de fichero debe comprobar cada 6 meses el correcto funcionamiento y aplicación de los procedimientos de copia de respaldo y la recuperación de la misma.
11	Medio	El sistema maneja dcp nivel medio. La última auditoría es de 2010	96.1	M	N	Realizar auditoria inmediatamente y con un periodo máximo de dos años
12	Alto	No se ha podido constatar que el RS haya traslado un informe con las conclusiones de la última auditoría al RF	96.3	M	N	Trasladar los resultados
13	Alto	Cuando un usuario se equivoca 20 veces al autenticarse, se bloquea.	98	M	S	
14	Básico	No se deja constancia de las recuperaciones de datos en el registro de incidencias.	100.1	M	N	Dejar constancia de las recuperaciones de datos
15	Alto	Los dcp de nivel alto no se cifran cuando los soportes salen del CPD	101.2	M	N	Cifrar esos datos ya que son de nivel alto y además salen del CPD
16	Alto	Las salvas se generan con original y copia y se almacenan en un armario ignífugo en el CPD	102	M	S	
17	Básico	Si el acceso a los dcp no tiene éxito, no se registra el intento de acceso	103.1	M	N	De cada acceso, fallido o no, se debe registrar 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
18	Alto	El administrador de sistemas puede desactivar el registro de accesos sin autorización del RF	103.3	M	N	Únicamente RS puede tener acceso a DCP

19	Básico	No se dispone de registro de acceso aunque el RF es la única persona que accede a los dcp	103.6	M	S	En caso de ser él la única persona física con acceso no debe dejar registros.
20	Básico	Las comunicaciones internas inalámbricas con dcp de nivel alto no se cifran	104	M	N	Cifrar las comunicaciones