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	Básico	No	Añadir el apartado c) del punto 3 (Funciones y obligaciones del personal)
2	Alto	El DS no incluye los procedimientos de copias de respaldo y de recuperación	88.3	Básico	No	Añadir el apartado f) del punto 3 (Copias de respaldo y recuperación)
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.	88.4 102	Alto	Si	Si se quiere mejorar la seguridad se puede incluir lo descrito en el apartado 4.b) (Controles periódicos)
4	Medio	El personal entrevistado desconoce las normas de seguridad	89.2	Básico	No	El responsable del fichero tendrá que adoptar las medidas necesarias para que se conozcan las normas de seguridad.

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	91.1	Básico	No	Crear claves con funcionalidades limitadas para que solo puedas acceder a los recursos que tienen que usar. Las claves deben restringir quienes tienen acceso a las aplicaciones para que alguien que no esté autorizado no pueda acceder a los servicios.
6	Básico	No se dispone de un inventario de soportes que contengan dcp	92.1	Básico	Quizás	Si bien es obligatorio llevar el inventario de soportes hay excepciones y no se sabe si las cumplen.
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	92.3 92.4	Básico	No	Los documentos deben ser destruidos de manera segura, no almacenados una vez pasa el plazo requerido.
8	Alto	Se ha constatado que los usuarios de un departamento comparten la misma contraseña	93.3	Básico	No	Se deben crear contraseñas únicas para cada usuario
9	Básico	El sistema obliga a cambiar las contraseñas de los usuarios administradores cada 12 meses	93.4	Básico	Si	Aunque el plazo es acertado se recomienda que se cambien cada menos tiempo para evitar problemas.
10	Medio	El RF no verifica cada seis meses el correcto funcionamiento de los procedimientos de salva y recuperación	94.3	Básico	No	El RF debe verificar cada seis meses el correcto funcionamiento de los procedimientos de salva y recuperación
11	Medio	El sistema maneja dcp nivel medio. La última auditoría es de 2010	96.1	Medio	No	Cada dos años tiene que hacerse una auditoria.
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	Medio	No	El RS tiene que trasladar las conclusiones al RF para que tome las medidas necesarias para subsanar los problemas
13	Alto	Cuando un usuario se equivoca 20 veces al autenticarse, se bloquea.	98	Medio	Si	20 intentos son muchos, se recomienda bajar los intentos a 5 para mejorar la seguridad.
14	Básico	No se deja constancia de las recuperaciones de datos en el registro de incidencias.	100.1	Medio	No	Llevar un registro de las recuperaciones de datos en el registro de incidencias.

15	Alto	Los dcp de nivel alto no se cifran cuando los soportes salen del CPD	101.2	Alto	No	Cifrar los datos personales y hacer que estos datos no sean accesibles.
16	Alto	Las salvas se generan con original y copia y se almacenan en un armario ignífugo en el CPD	102	Alto	Si	Las copias de seguridad deben almacenarse en una ubicación distinta para protegerlas de desastres que puedan ocurrir en la ubicación.
17	Básico	Si el acceso a los dcp no tiene éxito, no se registra el intento de acceso	103.1	Alto	No	Se debe registrar el intento de acceso para que sea revisado.
18	Alto	El administrador de sistemas puede desactivar el registro de accesos sin autorización del RF	103.3	Alto	Si	No permitir al administrador desactivar el registro de acceso sin la previa autorización del RF.
19	Básico	No se dispone de registro de acceso aunque el RF es la única persona que accede a los dcp	103.6	Alto	Si	Dejar constancia de esto en el documento de seguridad por si es necesario tomar acciones en un futuro.
20	Básico	Las comunicaciones internas inalámbricas con dcp de nivel alto no se cifran	104	Alto	No	Cifrar las conexiones internas ya que contienen datos sensibles.