Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Resumen Medidas Seguridad RD 1720/2007
Ficheros automatizados

	Nivel básico: ficheros o tratamientos de datos de carácter personal		
	Nivel medio: ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad		
	Nivel alto: ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género		
DOCUMENTO DE SEGURIDAD	- Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad - Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos - Identifica al encargado del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato - Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente	- Identifica al o los responsables de seguridad - Establece los controles periódicos de cumplimiento del documento	
RESPONSABLE DE SEGURIDAD		- Es el encargado de coordinar y controlar las medidas de seguridad del documento - Esto no supone exoneración de la responsabilidad del responsable del fichero	
AUDITORIA		- Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII - Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras - Es analizado por el responsable de seguridad - Queda a disposición de la AVPD	
PERSONAL	- El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado - Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento		
IDENTIFICACIÓN Y AUTENTICACIÓN	- Existen medidas para la identificación y autenticación de los usuarios - Se identifica unívoca y personalmente a cada usuario - Existe un procedimiento de gestión, almacenamiento y distribución de contraseñas - Existe un procedimiento para controlar la caducidad de contraseñas y el almacenamiento ininteligible de las mismas	- Se establece un mecanismo que limite el número de intentos reiterados de acceso no autorizado	
CONTROL Y REGISTRO DE ACCESOS	- Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones - Existe una relación actualizada de usuarios, perfiles y accesos autorizados - Existen mecanismos para controlar los derechos con que se accede a los recursos - Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad	- Se realiza un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información	- Se registran los datos de cada intento de acceso. - Los datos se conservan 2 años - Está bajo control del responsable de seguridad - El responsable de seguridad realiza un informe mensual - Existe una excepción: persona física y acceso unipersonal
GESTIÓN Y DISTRIBUCIÓN DE SOPORTES Y DOCUMENTOS	- Se identifica el tipo de información que contienen - Se mantiene un inventario - Se almacenan con acceso restringido - El responsable del fichero autoriza la salida de soportes - Se adoptan medidas en caso de desecho de soportes	- Existe un registro de entrada y salida de soportes que permite conocer el tipo de soporte o documento, la fecha y hora, el emisor o receptor, el tipo de información, la forma de envío y la persona responsable	- Existe un sistema de etiquetado solo comprensible para los usuarios autorizados - Se cifran los datos en la distribución de soportes y en los dispositivos portátiles
COPIAS DE RESPALDO Y RECUPERACIÓN	- Debe existir un procedimiento de copias de respaldo y recuperación de datos - El procedimiento garantiza la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción - Se realiza una copia de respaldo, al menos semanal - El responsable del fichero verifica semestralmente los procedimientos de copia - Se trabaja sólo con datos reales si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado y se ha hecho una copia		- Debe existir una copia de respaldo y de los procedimientos de recuperación en lugar diferente del que se encuentren los equipos
REGISTRO DE INCIDENCIAS	- Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados	- Se debe registrar la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y grabados manualmente - El responsable del fichero autoriza la ejecución de los procedimientos de recuperación de datos	
TELECOMUNICA-CIONES	- Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local		- La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada