AECEMCO

ASOCIACIÓN EMPRESARIAL DE CENTROS ESPECIALES DE EMPLEO

DOCUMENTO DE SEGURIDAD

21 de Mayo de 2019

INDICE

1.- OBJETO DEL DOCUMENTO DE SEGURIDAD DE AECEMCO

El presente documento y sus Anexos, están redactados en cumplimiento de lo dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos digitales (LOPD), y su normativa de desarrollo.

OBJETO DEL DOCUMENTO DE SEGURIDAD

Dotar AECEMCO, de las medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal que trata para la consecución de su misión, visión y valores y el cumplimiento de sus fines.

2.- AMBITO DE APLICACIÓN DEL DOCUMENTO

Este documento de seguridad ha sido elaborado bajo la responsabilidad de AECEMCO que, como Responsable del tratamiento de los Ficheros, se compromete a implantar y actualizar el mismo.

El documento será de aplicación a los tratamientos de los ficheros que contienen datos de carácter personal que se hallen bajo la responsabilidad de AECEMCO

Incluyendo los sistemas de información, soportes y equipos empleados para ello, así como a las personas contratadas que intervienen y a las dependencias en los que se ubican.

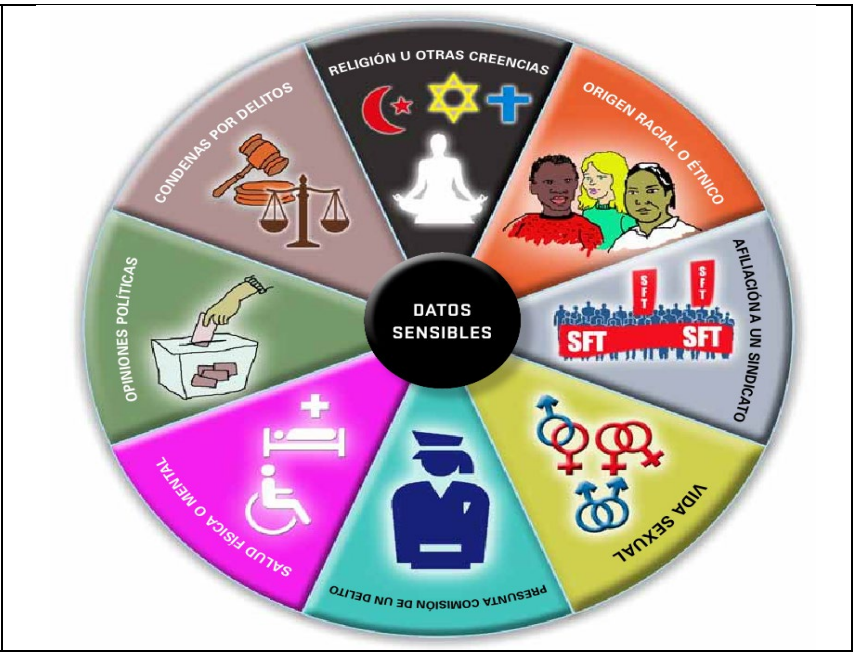
En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los establecidos en el Anexo I del Documento de Seguridad (Registro de Actuaciones de Tratamiento).

3.- RECURSOS PROTEGIDOS

TODOS LOS RECURSOS DE AECEMCO

- **Los locales y dependencias de AECEMCO** donde se ubiquen los sistemas de información que contienen ficheros con datos de carácter personal.
- **Los puestos de trabajo** locales (puestos de trabajo de servicios centrales) o remotos (servicios de integración laboral) desde los que se pueda tener acceso a datos.
- **Los servidores** informáticos y **los sistemas informáticos**, o aplicaciones de los mismos.
- **Los ficheros** temporales o definitivos.
- **Las bases de datos** que contengan datos de carácter personal.

4.- CLASIFICACION DE DATOS PERSONALES

DATO DE CARÁCTER PERSONAL Es cualquier información referente a personas físicas identificadas o identificables.	

TIPOS DE DATOS QUE SE TRATAN EN AECEMCO

DE CATEGORÍA NO ESPECIAL	DE CATEGORÍA ESPECIAL (SENSIBLES)
Casi todos corresponden a personas jurídicas, aunque en algunos casos se tratan datos identificativos (Nombre y apellidos, teléfono, DNI, correos electrónicos…), correspondientes a los miembros de órganos de gobierno, proveedores y solicitantes de servicios	**En algunas ocasiones se tratan datos de salud** (discapacidad) para la gestión de los servicios de accesibilidad

5.- CONTROL DE ACCESO A LAS INSTALACIONES DE AECEMCO

La puerta principal al centro de trabajo de AECEMCO, será el único punto de acceso. **Para el personal de AECEMCO** se habilitará un **sistema con parámetros biométricos** (huella dactilar). El acceso a las **áreas de acceso restringido** (Servidores y las Salas con ficheros en papel con datos personales) precisará, además de autenticación e identificación

AUTENTICACIÓN
comprobación de la identidad del usuario asignando una contraseña

IDENTIFICACIÓN
reconocimiento de la identidad de un usuario una vez introduce en el sistema la contraseña asignada

Las puertas de acceso a los ficheros, deben estar permanentemente cerradas o vigiladas

5.1- Vigilancia de las personas en los lugares con acceso restringido y visitas

VISITAS SIN ACCESO A DATOS PERSONALES:

Deben estar acompañados en todo momento y se vigilará que no accedan a áreas de acceso restringido.

Si acceden personas no autorizadas a las intalaciones de AECEMCO

se avisará al Responsable de Seguridad

LAS VISITAS CON ACCESO A DATOS PERSONALES

han de tener autorización excepcional para ello

5.2.- Sistema de videovigilancia

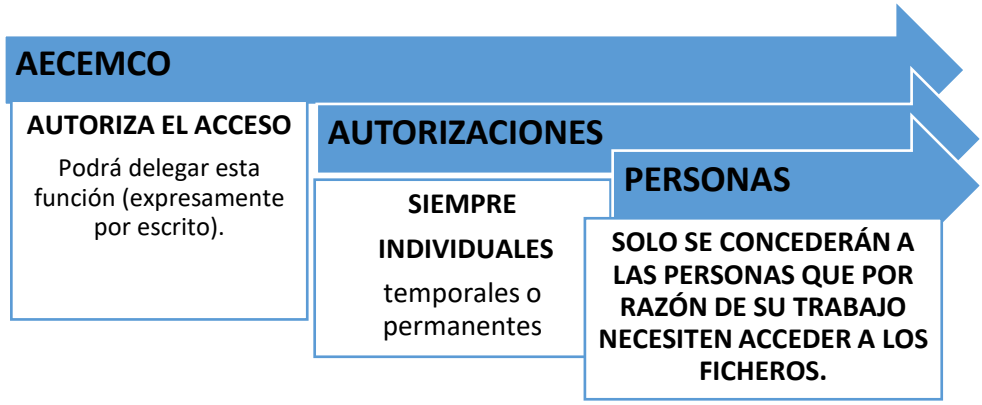
6.- CONTROL DE ACCESO A LOS DATOS PERSONALES

6.1.- Acceso con autorización

La autorización para uso de datos personales consiste en asignar a cada persona contratada que acceda a ellos una autorización para un uso concreto.

El Documento de Seguridad contiene un Registro de personal contratado autorizado con acceso a datos personales.

El personal autorizado, sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Al finalizar la relación laboral del personal contratado, procederá la devolución de todos los dispositivos que esté utilizando y se le dará de baja en el sistema de acceso a las dependencias de AECEMCO



6.2.- Acceso a ficheros no automatizados (formato papel)

LA PERSONA AUTORIZADA DEBE	➢ **Usar el menor número** de documentos en formato papel. ➢ **Mantener su puesto de trabajo despejado de documentos** que contengan datos personales para evitar que puedan ser vistos por terceras personas. ➢ **Custodiarlos e impedir el acceso de personal no autorizado** a los mismos, ➢ **Usar un sistema de etiquetado comprensible que impida conocer que el contenido tiene datos personales**. (ej.: códigos), solo conocido por él u otros autorizados. ➢ **Hacer solo las copias necesarias.** Archivar los documentos una vez se haya finalizado su uso y si no es necesario usarlos nunca más (y ha pasado el plazo legal de conservación) destruirlos en la destructora de papel.
PERSONAS EXTERNAS O NO AUTORIZADAS	➢ **Tienen que firmar** autorización excepcional **para su posible acceso al tratamiento** y siempre será para una ocasión determinada y para una única finalidad.

6.3.- Acceso a los ficheros automatizados (informatizados)

MECANISMO DE CONTROL DE ACCESO	➢ **Con contraseña** a los Ficheros con datos necesarios para el puesto ➢ **La solicitud de alta, baja o modificación de autorizaciones de acceso y contraseñas** la realizará por escrito el/la Responsable de Área al Responsable de Seguridad
ACCESOS POR PERSONAL EXTERNO	➢ Solo mediante autorización excepcional expresa y sometida a las medidas de seguridad aquí recogidas
ACCESO A DATOS POR CUENTA DE TERCEROS	➢ Es obligatorio realizar un contrato por escrito con las empresas externas o entidades que traten datos personales de AECEMCO

Existe un Registro de Accesos, supervisado por el Departamento Informático**,** en el que consta identificación, fecha y hora en que se realizó**,** el fichero al que se quiso acceder y si este ha sido autorizado o denegado**.** Con la información de control registrada se realizará un INFORME MENSUAL**.**

NO ESTÁ PERMITIDA, EN NINGÚN CASO,
DESACTIVAR EL MECANISMO QUE PERMITE EL REGISTRO DE ACCESOS

6.4. Controles de acceso a la sala de servidores y a copias de seguridad

Los sistemas de información, y los ficheros automatizados por ellos procesados, se encuentran en la Sala de Servidores, con puerta cerrada bajo llave y cuyo acceso está restringido al personal de AECEMCO mediante autorización.

El acceso a esta Sala por parte de personal externo o visitas debe estar justificado y documentado mediante el **Registro de acceso a la Sala de Servidores y copias de seguridad.**

Para asegurar la integridad y disponibilidad de los datos se realizan copias de seguridad y respaldo que permiten la recuperación de los datos personales en caso de fallo del sistema informático y se almacenan en la caja fuerte ubicado en el departamento de finanzas.

6.5. Accesos por razones de urgencia a todo tipo de ficheros

Razones de urgencia o fuerza mayor: acontecimiento extraordinario e imprevisible, y que no hubiera sido posible evitar aun aplicando la mayor diligencia **Las razones de urgencia o de fuerza mayor han de** notificarse como incidencia para su constancia en el **Registro de Incidencias**.

ACCESO POR PERSONAL NO AUTORIZADO POR RAZONES DE URGENCIA O FUERZA MAYOR

*** Cumplimentar ficha** "Autorizaciones excepcionales"
*** Acceso físico:** siempre acompañados del Responsable de Área
***Acceso electrónico:** en presencia de la persona autorizada para el acceso (el titular de la contraseña y usuario que así lo permiten))

7.- GESTIÓN DE SOPORTES Y DOCUMENTOS

Un soporte es todo accesorio o dispositivo que posibilita el **almacenamiento** o la **transmisión** de datos.

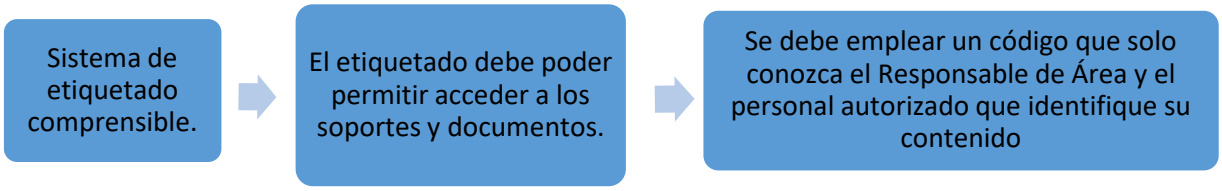
7.1.- El inventario de soportes

Todos los soportes que contengan datos de carácter personal han de ser inventariados. El inventario de soportes es gestionado por el/la Responsable de Seguridad.

EL PERSONAL DE AECEMCO ESTÁ OBLIGADO A CUSTODIAR LOS SOPORTES QUE LE HAYAN SIDO ASIGNADOS
(Independientemente de su formato), y a adoptar las medidas necesarias para mantener su seguridad.
La falta de diligencia se sancionará conforme a lo previsto en el XV Convenio Colectivo General de Centros y Servicios de Atención a Personas con Discapacidad

7.2.- Criterios de archivo y almacenamiento de soportes manuales con datos personales (ficheros no automatizados en formato papel)

Hay que tender a la digitalización de todos los documentos en formato papel para la eliminación progresiva de este tipo de ficheros. En aquellos que aún no se haya producido (o sea imposible) se seguirá el siguiente procedimiento de archivo:



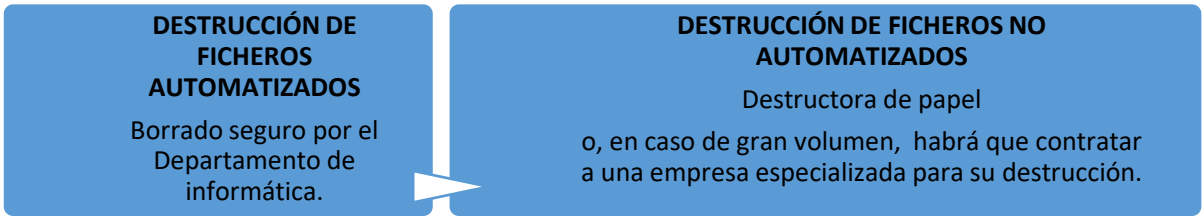
7.3.- Desechado y reutilización de soportes

Un Fichero habrá cumplido su finalidad o habrá caducado cuándo:

- La información se dispone repetida en otros soportes alternativos.
- La información se almacenaba para un uso esporádico o ha quedado desactualizada.
- La información o los archivos utilizados ya han cumplido su finalidad, etc.

En todo caso, los soportes se destruirán o reutilizaran siempre y cuando haya pasado el plazo legal de conservación.

¿QUIÉN PROCEDE AL BORRADO DE LOS DATOS PERSONALES?
El personal autorizado para desechar o reutilizar un soporte que contenga datos personales y SIEMPRE INFORMANDO DE ELLO al Responsable de Seguridad



REUTILIZACIÓN DE SOPORTES AUTOMATIZADOS

7.4.- Registro de entrada y salida de soportes

NO SE PUEDEN LLEVAR A CABO TRATAMIENTOS DE DATOS PERSONALES FUERA DE LAS DEPENDENCIAS, de AECEMCO, mediante soportes automatizados o no

SALVO CASOS EXCEPCIONALES O EVENTOS Y SERÁ NECESARIA AUTORIZACIÓN

Petición por escrito al Responsable de Seguridad, justificando la necesidad de disponer de esos ficheros. Especificando quién accede a los datos, que datos son si están cifrados, etc

SOLO SE UTILIZARÁN LOS DATOS NECESARIOS Y SE COMUNICARÁ EL FIN DE SU USO

También se realizara en el caso de que exista un encargado del tratamiento que así lo precise y si así está reflejado en un contrato

La salida de soportes automatizados y dispositivos portátiles = siempre bajo sistema de cifrado

7.5.- Acceso y envío de datos a través de redes de comunicación

AECEMCO

No cuenta con un acceso genérico a los ficheros que contengan datos personales almacenados en el servidor, para toda la plantilla.

El RESPONSABLE DE SEGURIDAD Y EL PERSONAL TÉCNICO AUTORIZADO SON LOS ÚNICOS QUE ACCEDAN A DATOS PERSONALES

ESTÁN PROHIBIDOS

- LOS ACCESOS REMOTOS
- LOS ENVÍOS POR REDES INALÁMBRICAS
- LOS ENVÍOS POR RED DE COMUNICACIÓN

El envío de datos por correo electrónico = siempre bajo autorización y encriptados

Envío de datos en papel a terceros = siempre con autorización y en sobre cerrado, Por correo certificado o mediante forma de correo ordinario que permita su completa confidencialidad

7.6- Medidas durante los traslados de documentación

FICHEROS AUTOMATIZADOS

- **Impedir el acceso o manipulación de la información** objeto de traslado, (Se añadirán contraseñas, etc…)
- Autorización **y Sistema de registro de entrada y salida de soportes**: Indicar: Tipo de documento o soporte, la fecha y hora, emisor o destinatario,número de documentos o soportes incluidos en el envío...

FICHEROS NO AUTOMATIZADOS

- Autorización, previa explicación y justificación del traslado. Se hará constar en la autorización la fecha prevista para el traslado y el lugar de destino de dicha documentación, junto con la persona que se va a hacer responsable de la custodia de la misma.

7.7.- Ficheros temporales (copias de trabajo de documentos)

FICHEROS AUTOMATIZADOS

SOLO SE PERMITIRÁ LA CREACIÓN DE FICHEROS TEMPORALES O COPIAS DE DOCUMENTO, POR PERSONAL AUTORIZADO

SI SON GENERADOS AUTOMÁTICAMENTE EN PROCESOS INTERNOS

Se custodiarán por la persona autorizada.

Si se producen fallos en su uso se analizarán por el Dto. Informática.

CUMPLIDA SU FINALIDAD: SE DEBEN DESTRUIR.

(Automáticamente. Dto. Informática o programa informático).

No se podrán almacenar de manera indefinida.

FICHERO NO AUTOMATIZADO O EN PAPEL

SOLO SE PERMITIRÁ LA CREACIÓN DE FICHEROS TEMPORALES O COPIAS DE DOCUMENTO EN PAPEL por personal autorizado (Informando siempre al Responsable de área y al Responsable de Seguridad).

LAS COPIAS QUE SE REALICEN, se harán bajo control directo del Responsable del Área. No se permite el traslado fuera de AECEMCO sin la autorización del Responsable de Área y Responsable de Seguridad.

CUMPLIDA SU FINALIDAD: SE DEBEN DESTRUIR. (Procedimiento establecido destructora de papel o empresa con contrato y certificación de destrucción si hay gran volumen de copias).

7.8.- Copias de respaldo y recuperación de ficheros automatizados

COPIA DE RESPALDO

Es la copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Tendrá carácter **obligatorio.**

Se realizará 1 vez al mes cuando los sistemas de información y ordenadores de plantilla no estén activos

CONSERVAR LAS COPIAS DE RESPALDO

Se conservarán en los servidores de AECEMCO

Una vez cerrado el año, se realizará una copia que se etiquetará como copia anual y se almacenará durante 5 años.

SE REALIZARÁN POR:

Departamento de informática y persona autorizada con acceso directo al Servidor.

Gestión: Dto. Informática con Supervisión del Responsable de Seguridad

7.9.- Recuperación en caso de incidencia o pérdida de datos

Incidencia detectada

- Comunicación por la persona autorizada al Responsable de Seguridad.

Análisis

- Se decide conjuntamente por el responsable qué contenido debe recuperarse y cómo

Notificación

- Dto. Informática: Analizará el fallo, elaborará informe técnico, identificará los archivos a recuperar y se guardarán en otra ubicación con copia encriptada.
- Será **notificada como INCIDENCIA**

7.10.- La destrucción de ficheros

DESTRUCCIÓN DE DOCUMENTACIÓN DE FICHEROS NO AUTOMATIZADOS (PAPEL). Se puede:

- **Subcontratar a una empresa especializada en destrucción de papel** que garantice la seguridad de la documentación en su transporte y la confidencialidad durante todo el proceso. La empresa **debe proporcionar a AECEMCO un Certificado de destrucción**.

- **Triturar el papel** con la trituradora de papel de la oficina (capaz de también la destrucción de otro tipo de soportes tales como CD´S), de hoja en hoja, de forma talque no permita su reconstrucción. Después, los restos de papel pueden arrojarse al contenedor normal de reciclado de papel.

DESTRUCCIÓN DE FICHEROS AUTOMATIZADOS, el Dto. De Informática, borrará o formateará el soporte.

Con la destrucción del fichero se dará su baja en el Registro de actividades de tratamiento
Y en el Registro de soportes y respaldos

8.- RECURSOS INFORMÁTICOS

8.1–Uso de recursos informáticos

NO ESTÁ PERMITIDO

El uso de recursos para **FINES PERSONALES**

INSTALAR aplicaciones, programas, macros, etc que puedan dañar los datos personales

DESACTIVAR programas antivirus

COPIAR datos personales en pen drives, cd,s discos duros, etc. si estos no tienen las medidas de seguridad necesarias

DESTRUIR, ALTERAR O INUTILIZAR programas o documentos que puedan afectar a datos personales (Delito de daños informáticos artículo 264 del Código Penal)

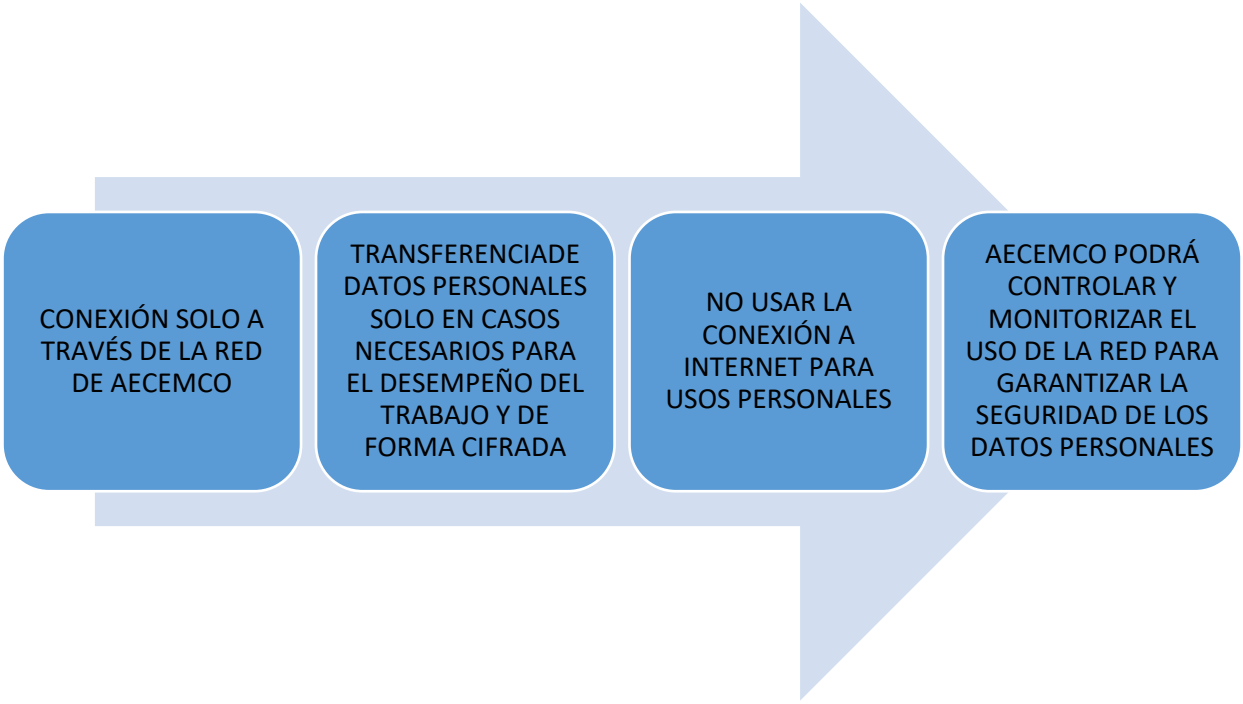
INTRODUCIR en los sistemas de información o la red de AECEMCO contenidos obscenos, amenazadores, inmorales u ofensivos

INTENTAR DESCIFRAR LAS CLAVES, sistemas o algoritmos de cifrado, u otro tipo de medidas de seguridad

CONECTARSE A LA RED O A INTERNET A TRAVÉS DE OTROS MEDIOS que no sean los definidos y administrados por AECEMCO.

8.2.-Conexión a internet

LA AUTORIZACIÓN DE ACCESO A INTERNET Se concede por el Departamento de Informática



18.3.- Correo electrónico y aplicaciones de mensajería

USO DEL CORREO ELECTRÓNICO	➢ Exclusivamente **para fines profesionales**. No está permitido: ▪ Leer, borrar, copiar o modificar los mensajes de correo electrónico de otras personas usuarias sin autorización expresa. ▪ El envío de comunicaciones publicitarias o promocionales.
PRECAUCIONES	➢ Enviar los correos con copia oculta si el envío es múltiple. ➢ Si se remiten datos personales por correo electrónico han de cifrarse. ➢ Utilizar solo las aplicaciones preinstaladas y autorizadas por AECEMCO.
REVISIONES DE CORREO ELECTRÓNICO	**Los correos se supervisarán por el Responsable de Seguridad** para evitar que pueda afectar a los sistemas de seguridad de los datos personales de AECEMCO.

8.4- Política de contraseñas

Solo serán conocidas por la persona contratada y por el Departamento de Informática.

Cambio de contraseñas en el caso de que se produzcan incidencias

Estará compuesta de identificador de usuario y contraseña.

Serán siempre mayúsculas, minúsculas, números, letras y caracteres especiales de entre 8 y 12 caracteres.

En el caso de cuentas de correo el sistema las generará automáticamente

Cambio de contraseñas anual

Cambiar las contraseñas por defecto proporcionadas por fabricantes

El Departamento de informática CUSTODIARÁ la relación de contraseñas estableciendo medidas de seguridad para que estas sean ininteligibles

Los accesos no autorizados se notificaran como incidencias

Contraseñas Seguras

- No utilizar siempre la misma contraseña.
- Evitar utilizar información personal, las repeticiones de caracteres, las secuencias básicas de teclado o de números, utilizar la misma contraseña siempre en todos los sistemas o servicios. (ej. qwer",-1234).
- No escribir ni reflejar la contraseña en documento donde quede constancia de la misma o guardar en documentos de texto dentro del propio ordenador o dispositivo.
- No enviar la contraseña por correo electrónico o SMS o mencionar en una conversación.

9.- CENTROS DE TRABAJO Y EQUIPAMIENTO

Para cumplir con la Política de Seguridad de COCEMFE, se han establecido las siguientes medidas de seguridad para impedir el acceso no autorizado a sus centros de trabajo:

9.1.- Sistemas de control de accesos

EDIFICIO

- El centro tiene una vía de entrada y una salida de emergencia independientes.
- Sistema de control de acceso presencial en la puerta principal (recepción vigilada)
- Al interior de las instalaciones mediante identificación biométrica (huella dactilar)
- En todas las instalaciones hay instalado un sistema de videovigilancia
- Los soportes no automatizados se encuentran ubicados en armarios protegidos con cerradura.

CUARTO DE SERVIDORES

- La sala de servidores está en cuarto protegido con cerradura
- Para acceder a la sala se de servidores hay que hacerlo a través de otra sala también protegida por cerradura.

9.2.- Sistemas de detección

EDIFICIO Se cuenta con sistemas de detección de incendios en las instalaciones, así como de extintores en todas y cada una de las salas

CUARTO DE SERVIDORES Se cuenta con sistemas de detección de incendios así como de extintor y sistema específico de refrigeración

9.3.- Equipamiento

- Se cuenta con extintores de incendios en todas las salas (incluida la sala de servidores).
- La sala de servidores cuenta con sistema de refrigeración independiente de los equipos

10.- CLASIFICACION DEL PERSONAL AFECTADO POR EL DOCUMENTO DE SEGURIDAD:

RESPONSABLE DEL TRATAMIENTO (FICHEROS)

Persona física y/o jurídica, que decide sobre el tratamiento de los datos durante todo su ciclo de vida y los usos de la información

AECEMCO

Puede hacer Delegación de funciones y Responsabilidades

ENCARGADO DE TRATAMIENTO

Persona física o jurídica que presta un servicio a AECEMCO que conlleva el tratameinto de datos personales

PUEDE SER AECEMCO/EMPRESA EXTERNA/ENTIDAD DE AECEMCO

Si no es AECEMCO tiene que existir **un contrato de tratamiento de datos**

que fije las obligaciones y responsabilidades

Si ya existía un Contrato de Tratamiento de datos anterior, hay que añadir **la Addenda a los contratos formalizados con terceros** para incluir las nuevas obligaciones que marca el RGPD

RESPONSABLE DE SEGURIDAD

Se designa por 4 años y coordina y controla las Medidas de Seguridad

ADMINISTRADORES

Personal informático encargado de administrar o mantener el entorno operativo del fichero

PERSONAL CONTRADO

Autorizado a acceder a datos personales

OTRAS PERSONAS

Con **autorización excepcional** para acceder de forma ocasional a datos personales

10.1- Funciones y obligaciones específicas del encargado del tratamiento

10.2.- Funciones y obligaciones específicas del responsable de seguridad

Su principal función es coordinar y controlar las medidas definidas en el Documento de Seguridad, además de cualesquiera otras que pueda delegarle AECEMCO (Responsable del Tratamiento).

RECURSOS PROTEGIDOS Y MEDIDAS DE SEGURIDAD	➢ **Implantar controles periódicos de cumplimiento** del Documento de Seguridad. ➢ **Crear y Mantener cuantos inventarios y Registros corresponda** en virtud del Documento de Seguridad.
CONTROL DE ACCESO A DATOS PERSONALES	➢ **Mantener actualizada y controlar la lista del personal contratado en el Documento de Seguridad** así como las autorizaciones de acceso y autorizaciones para hacer copias. (Datos de categoría especial o no especial). ➢ **Adoptar las medidas oportunas para el personal ajeno a AECEMCO** que tenga acceso a los ficheros no automatizados esté sometido a las mismas condiciones y obligaciones de seguridad que el personal propio. ➢ **Confeccionar y mantener el listado con la relación de empresas externas** con acceso a datos personales y **Verificar la firma de** contratos con los Encargados de Tratamiento.
GESTIÓN DE SOPORTES Y DOCUMENTOS	➢ **Establecer un sistema de archivo para soportes y documentos** que garanticen su correcta conservación, localización, consulta e información. ➢ **Confeccionar y mantener los siguientes Registros:**

	▪ Inventario de ficheros y actividades de tratamiento. ▪ Inventario de Soportes (automatizados y no automatizados). ▪ Registro de Ubicación de soportes. ➢ **Controlar que solo el personal autorizado accede a ficheros no AUTOMATIZADOS**. (PAPEL) y que su ubicación este protegida con llave o sistema adecuado y en áreas cerradas. ➢ **Controlar que solo realicen copias de los datos personales las personas autorizadas** para ello. ➢ **Realizar y cumplir un procedimiento de destrucción de soportes y de copias desechadas** que contengan datos de categoría especial. ➢ **Vigilar que los traslados de archivos físicos** se realicen tomando las medidas establecidas en el presente documento. ➢ **Establecer un sistema para IDENTIFICAR el almacenamiento de FICHEROS TEMPORALES** (indefinido o no) y para revisarlo periódicamente.
FUNCIONES DE PERSONAL	➢ **Informar y formar al personal** para que conozcan las normas de seguridad para que puedan implantarlas y sus consecuencias en caso de incumplimiento
RECURSOS INFORMATICOS	➢ **Adoptar las medidas necesarias para que los accesos a datos personales no queden fuera de control.** ➢ **Crear y mantener los siguientes Registros:** ▪ Registro de Hardware empleado en AECEMCO ▪ Registro de Software empleado en AECEMCO
INCIDENCIAS	➢ **Crear y gestionar un sistema de Gestión De Incidencias** estableciendo un Registro para ello. (Que contenga tipo de incidencia, momento en que se ha producido, efectos, etc.).
EJERCICIO DE LOS DERECHOS DE PERSONAS USUARIAS	➢ **Crear y gestionar un sistema que contendrá la forma de ejercitar los derechos de los ciudadanos y ciudadanas** a criterio de AECEMCO. ➢ **Tienen que conocer y registrar todas las solicitudes de ejercicio de los derechos,** motivando, en su caso su denegación. ➢ **Debe de solicitar, en su caso, a terceros encargados del tratamiento que procedan a ejercer el derecho solicitado** y en caso de omisión notificarlo a la AEPD.
REVISIÓN DEL DOCUMENTO DE SEGURIDAD	➢ **Someter los sistemas de información, al menos cada 2 años, a una auditoría** interna o externa y analizar la misma para informar a AECEMCO por si hubiese que implantar medidas correctoras

10.3.- Funciones y obligaciones específicas de los administradores o personal informático

CLASIFICACIÓN DE LOS ADMINISTRADORES Y PERSONAL INFORMÁTICO

ADMINISTRADORES	OPERADORES	PERSONAL DE MANTENIMIENTO DE LOS SISTEMAS
•Son la máxima autoridad y tienen acceso al software del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarias para resolver los problemas que surjan.	•Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles.	•Personal responsable de la resolución de incidencias que puedan surgir en el entorno hardware/sortware de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

OTRO PERSONAL INFORMÁTICO QUE LA ORGANIZACIÓN ESTABLEZCA

Las pruebas para la implantación o modificación de sistemas de información que traten datos personales no se deben de realizar con datos reales y queda prohibido el uso de programas informáticos sin la correspondiente licencia.

Características de los ordenadores

- Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a personas usuarias o administradores no autorizado.

- **Los administradores deben cuidar de que los mecanismos que permiten el registro de accesos estén bajo el control directo del Responsable de Seguridad.** De cada acceso se guardarán, siempre que sea posible, 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. También habrán de controlar los intentos de acceso fraudulento al Fichero.

AECEMCO (Responsable del Fichero)
Concederá, alterará o anulará el acceso autorizado.
En caso de baja o cese en AECEMCO de personal contratado
Se dará de baja el CÓDIGO DE USUARIO.

10.4.- Funciones y responsabilidades del personal de AECEMCO

Con carácter general, todo el personal de AECEMCO tiene las siguientes responsabilidades:

CONOCER	•Y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.
UTILIZAR	•Los sistemas de información, recursos técnicos así como la información personal a la que se accede, únicamente para el desarrollo y desempeño de sus funciones.
NOTIFICAR	•las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos.
FACILITAR	•El ejercicio de los derechos reconocidos en la normativa de protección de datos, a las personas titulares de los mismos.
GUARDAR	•Secreto profesional y confidencialidad de la información tratada. Obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del Fichero o, en su caso, con el Responsable del mismo.

No se permite la distribución de datos de carácter personal de ninguna clase
Fuera de las instalaciones de AECEMCO.
Salvo excepciones o eventos concretos excepcionales que así lo requieran
Y con autorización expresa.

LA VULNERACIÓN DEL DEBER DE GUARDAR SECRETO
Será considerada como una falta leve, grave o muy grave, de conformidad con lo previsto en el Convenio Colectivo de aplicación en AECEMCO, o en la normativa legal vigente, motivo por el cual puede dar lugar al inicio de actuaciones disciplinarias si procediese

En relación con su actividad y puesto de trabajo, todo el personal deberá observar las siguientes medidas de seguridad

CONTRASEÑAS	➢ **Utilizar la contraseña** facilitada por el Dto. Informática para acceder al ordenador ubicado en su puesto de trabajo y responsabilizarse de su confidencialidad. ➢ Si ocurriese alguna incidencia con la misma deberá comunicarlo al Responsable de Seguridad.
PUESTOS DE TRABAJO	➢ **Garantizar que la información que maneja no es visible** por personas no autorizadas. (Bloqueando su terminal durante las ausencias, etc…).
PERIFÉRICOS	➢ **Ubicar** las pantallas, las impresoras y otros dispositivos en lugares que garanticen confidencialidad. ➢ **Imprimir en "Modo seguro"** si se trata de datos personales y **asegurarse de que no quedan documentos impresos en la bandeja de salida con datos personales** ➢ **No conectarse desde los puestos de trabajo a redes o sistemas exteriores**, que no estén autorizado expresamente por el Departamento de Informática. ➢ **No cambiar la configuración fija de sus aplicaciones o sistemas operativos** (salvo autorización expresa).
ARCHIVOS TEMPORALES	➢ **Mantener controlados e identificados los ficheros existentes** ➢ **No hacer copias o tratar de datos extraídos del Fichero**, con programas ofimáticos, sin autorización. Si lo hace podrá instruirse expediente disciplinario. ➢ **Responsabilizarse de la custodia de archivos temporales** y realizará los mismos **sobre un mismo directorio** para evitar su dispersión y no almacenar los mismos de manera indefinida
INCIDENCIAS	➢ **Comunicar** a la mayor rapidez posible cualquier incidencia al Responsable de Seguridad. En Caso de no hacerlo puede incurrir en responsabilidades (posibilidad de expediente disciplinario).
COMUNICAR AL RESPONSABLE	➢ La reutilización, desechado de soportes, entrada y salida de los mismos y recuperación de ficheros y soportes.
SECRETO PROFESIONAL	➢ **Todo el personal de AECEMCO debe guardar secreto profesional y** confidencialidad de la información tratada durante su relación laboral e incluso después de finalizar esta.

.10.5.- Funciones y obligaciones específicas del personal de recursos humanos

PROCESOS DE SELECCIÓN	➢ **Recabar de los postulantes a los procesos de selección el** consentimiento expreso para el tratamiento de su CV.
DURANTE LA RELACIÓN LABORAL **Ha de asegurar que todo el personal contratado**	➢ **Ha prestado consentimiento expreso** para: ▪ El uso de sus datos personales. ▪ Para el uso de fotografías. ▪ Para el tratamiento de sus datos biométricos (huella dactilar). ➢ **Se le ha** comunicado la existencia del sistema de video vigilancia. ➢ **Ha firmado el** documento de confidencialidad. ➢ **Dispone** de: ▪ La guía de protección de datos personales. ▪ El código de conducta de personal. ▪ Copia de lectura fácil del Documento de Seguridad (solo si es personal autorizado al tratamiento de datos personales de carácter especial).
EL PERSONAL VOLUNTARIO	➢ **Ha firmar los mismos documentos que el personal contratado,** y se le entregará una copia del documento de seguridad.

10.6. Integrantes de los órganos de gobierno

Los integrantes de los órganos de gobierno de AECEMCO en su condición de la representación que ostentan y en el desempeño del puesto que ocupan en los mismos, tienen que acceder a documentos en papel y/o bases de datos automatizadas que contienen informaciones de carácter relevante y datos de carácter personal de distintos colectivos de personas que guardan relación con la Asociación y/o ficheros que los contienen y que son titularidad de AECEMCO.

Con base en ello vendrán obligados a conocer y cumplir las medidas adoptadas en el presente documento de seguridad y a **guardar confidencialidad y el secreto de las deliberaciones de los Órganos de los formen parte**, así como de toda aquella información a la que hayan tenido acceso en el ejercicio de su cargo, que utilizarán exclusivamente en el desempeño del mismo y que custodiarán con la debida diligencia. La obligación de confidencialidad y el deber de secreto subsistirá aún después de haber cesado en las funciones que le habilitaron el acceso.

10.7.- Otras personas

Personas ajenas que por motivo de su desempeño profesional, pueden tener acceso a la información de carácter personal.

La relación con estas empresas o personas externas a AECEMCO, la duración de sus funciones, así como los ficheros a los que tienen acceso quedarán reflejados en este Documento.

11.- LAS BRECHAS DE SEGURIDAD: PROCEDIMIENTO DE NOTIFICACIÓN, GESTION Y RESPUESTAS ANTE LAS INCIDENCIAS

UNA INCIDENCIA DE SEGURIDAD
Es cualquier incumplimiento de las normas del Documento de Seguridad o anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de AECEMCO

11.1.- Tipos de incidencias que pueden afectar a los datos personales

TÉCNICA	**Por un fallo en el sistema software o hardware.** Se debe solicitar soporte técnico al departamento de informática, para aplicar medidas correctoras.
DE GESTIÓN	**Por un error o carencia en la transcripción de Información.** Se subsanará recabando la información necesaria, por medio del personal que ha tenido acceso a los datos.

11.2- Procedimiento de notificación de incidencias

Detectada una incidencia de seguridad (pérdida de datos, acceso no autorizado, etc...) el personal contratado debe COMUNICARLO inmediatamente al Responsable de Seguridad.

La persona a cuyo cargo este el FICHERO DE DATOS personales (tras conocer la incidencia) debe intentar SUBSANARLA en CONSENSO con el Responsable de Seguridad.

El procedimiento de solución de incidencias debe ser conocido por todo el personal.

El conocimiento y la no notificación o registro de una incidencia
Por parte de un trabajador/a será considerado como una falta contra la seguridad del Fichero.

PROCESO DE RESPUESTA ANTE UNA INCIDENCIA

11.3.-El registro de incidencias:

Preferiblemente será en formato informático, puede ser también en papel y se revisará anualmente por el Responsable de Seguridad.

CONTENIDO

- El tipo de incidencia.
- La fecha y hora en la que ha ocurrido.
- La persona que realiza la notificación u a quien se lo comunica.
- Efectos de la misma.
- Procedimiento de recuperación da datos si así ha sido necesario.
- Soluciones o medidas correctoras adoptadas.

11.4.- Notificación a la agencia española de protección de datos

Si la incidencia ha afectado a datos personales,
hay que notificarlo a la Agencia de Protección de Datos
especialmente si la violación o incidencia,
pudiera afectar "a la intimidad o a los datos personales del interesado/a"

Cuando la incidencia, además, pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, el Responsable del tratamiento deberá comunicar a los afectados a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la AEPD.

La notificación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el Responsable considere adecuado.

La notificación indirecta, (a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa), se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo porque se desconocen, o los datos de contacto no están actualizados).

12.- LOS DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES: PROCEDIMIENTO PARA SU EJERCICIO

EL PERSONAL AUTORIZADO A TRATAR DATOS PERSONALES, DEBE CONOCER QUE

- Los Datos solo podrán utilizarse para una finalidad determinada.
- Su recogida debe ser proporcional a la finalidad para la cual se van a utilizar los datos.
- Si es preciso, se empleará un sistema de pseudónimos para la protección de los datos personales.
- Todos los ficheros se suprimirán cuando haya desaparecido la finalidad que motivó la recogida.
- Todos los contratos suscritos por AECEMCO deberán ser revisados y deberán adaptarse a la nueva normativa del Reglamento General Europeo de protección de datos. (RGPD).

AECEMCO DEBE INFORMAR A LA PERSONA TITULAR DE LOS DATOS PERSONALES QUE SE RECABAN DE LO SIGUIENTE

LA IDENTIDAD DE QUIÉN RECABA SUS DATOS PERSONALES.

QUE A SUS DATOS PERSONALES, SE LES ASIGNARÁ UN PSEUDÓNIMO EN LOS CASOS NECESARIOS

QUE SUS DATOS PERSONALES SE INCORPORARAN A UN FICHERO.

LA FINALIDAD DEL FICHERO DE DATOS PERSONALES EN EL QUE FIGURAN SUS DATOS

QUIÉNES SON LOS DESTINATARIOS DE LA RECOGIDA DE SUS DATOS PERSONALES

CÓMO Y DÓNDE EJERCER SUS DERECHOS

QUE SI SE PRODUCE UNA VIOLACIÓN DE SEGURIDAD QUE AFECTE A SUS DATOS PERSONALES AECEMCO SE LO COMUNICARÁ INMEDIATAMENTE Y ADOPTARÁ LAS MEDIDAS DE SEGURIDAD NECESARIAS

QUE UNA VEZ QUE SE RECABEN SUS DATOS PERSONALES, AECEMCO ESTARÁ OBLIGADO A ADOPTAR UNA SERIE DE MEDIDAS DE SEGURIDAD, DE CARÁCTER TÉCNICO Y ORGANIZATIVO PARA PROTEGER SUS DATOS (CONFIDENCIALIDAD, ETC)

QUE NO SE LE DARÁ DE ALTA EN NINGÚN SERVICIO DE AECEMCO SIN SU CONSENTIMIENTO EXPRESO (LOS CONSENTIMIENTOS TÁCITOS DESAPARECEN).

QUE PUEDE REVOCAR SU CONSENTIMIENTO EN CUALQUIER MOMENTO Y, ADEMÁS, DE FORMA SENCILLA Y GRATUITA.

12.1.- Derechos que pueden ejercitar las personas respecto de las que AECEMCO recaba datos personales:

DERECHO DE ACCESO	**Derecho a conocer qué datos de carácter personal están siendo tratados**, la finalidad de este tratamiento, el origen de los datos y si se han comunicado o se van comunicar a un tercero. No es necesario justificar el ejercicio de este derecho si no se ha ejercido en los últimos 12 meses.
DERECHO DE OPOSICIÓN	**Derecho a oponerse a que se realice el tratamiento de sus datos personales** en los casos que nos es preciso recabar el consentimiento previo, o que los ficheros se usen con fines publicitarios o que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado. **Para ejercitar este derecho, deberán hacerse constar los motivos fundados y legítimos**, que justifiquen el ejercicio de este derecho.
DERECHO DE RECTIFICACIÓN	**Permite a la persona afectada solicitar la modificación de datos que sean inexactos o incompletos.** **Para ejercitar este derecho** debe indicarse qué datos son los referidos y su corrección, aportando documentación justificativa.
DERECHO DE CANCELACIÓN	**Derecho a cancelar sus datos personales si estos son inadecuados o excesivos** Los datos no se eliminan directamente. **Se conservarán bloqueados** para la atención de las posibles responsabilidades que hayan surgido del tratamiento durante su plazo de prescripción. **Para ejercer este derecho** debe indicarse el dato a cancelar y el motivo, aportando documentación justificativa de la rectificación solicitada. **Si los datos han sido comunicados a un tercero**, se comunicara a su vez al mismo que estos datos deben ser cancelados.
DERECHO AL OLVIDO	**Derecho a que sus datos personales sean eliminados de los proveedores de servicios de internet**, siempre y cuando quien posea esos datos no tenga razones legítimas para retenerlos (que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones). **Si se ha difundido la información a terceros**, se les debe comunicar la obligación de suprimir enlaces a los datos publicados y copias de los mismos.
DERECHO A LA PORTABILIDAD	**Derecho a que se transmitan los datos de un Responsable a otro**, directamente cuando sea técnicamente posible (portabilidad). **Este derecho no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público** o en el ejercicio de poderes públicos conferidos al responsable.
DERECHO A NO SER OBJETO DE DECISIONES AUTOMATIZADAS	Incluye la elaboración de perfiles. **Este derecho no será aplicable cuando haya mediado previo consentimiento expreso, sea** necesario para la celebración o ejecución de un contrato entre el titular de los datos y responsable o el tratamiento esté autorizado por el Derecho de la UE.

DERECHO DE LIMITACIÓN DEL TRATAMIENTO	**Derecho a obtener del Responsable del Fichero la limitación del tratamiento de los datos durante el ejercicio del derecho de oposición o del derecho de rectificación** hasta que se resuelvan ambos.
DERECHO DE SUPRESIÓN	**Derecho a obtener la supresión de los datos personales que le conciernan,** cuando: ➢ Los datos personales ya no sean necesarios, o hayan sido tratados ilícitamente, o se hayan obtenido en relación con la oferta de servicios de la sociedad de la información. ➢ El interesado retire el consentimiento en que se basa el tratamiento o se oponga al mismo. ➢ Los datos personales deban suprimirse para el cumplimiento de una obligación legal Derecho de la Unión o de los Estados miembros. **AECEMCO se puede oponer a la supresión** ➢ Cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. ➢ Por razones de interés público, en el ámbito de la salud pública. ➢ Con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos. ➢ Para la formulación, el ejercicio o la defensa de reclamaciones.

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de la normativa de protección de datos
tendrá derecho a solicitar judicialmente a AECEMCO, como Responsable (o en su caso al encargado del tratamiento) una indemnización por los daños sufridos.

12.2.-Procedimiento para el ejercicio de derechos

PRESENTACIÓN Y TRAMITACIÓN DE LA SOLICITUD	AECEMCO C/ Luis Cabrera 63 - 28002 - Madrid aecemco@cocemfe.es (Ref. LOPD) - Teléfono: 91 744 36 00 – 637 887 283 Horario de atención al público: de 9:00 a 15:00 horas los días laborales
CONTENIDO DE LA SOLICITUD	➢ Nombre, apellidos del interesado y domicilio a efectos de notificaciones ➢ Fotocopia del DNI, NIE, Pasaporte, así como el documento acreditativo de la representación en su caso. ➢ La petición y documentos acreditativos de la misma. ➢ Fecha y firma del solicitante. **En caso que la solicitud no contemple la información requerida**, el responsable deberá requerir al interesado que, en un plazo de **quince días hábiles**, subsane la falta o acompañe los documentos necesarios.
MOTIVOS DE RECHAZO DE	➢ Ser presentada por una persona jurídica o por persona no titular (o representante legal) de los datos de carácter personal.

LA SOLICITUD	➢ Cuando se haya ejercitado el derecho de acceso en los últimos doce meses, salvo que se acredite un interés legítimo. ➢ En caso del derecho de rectificación cuando no se indique el dato que es erróneo y la corrección que debe realizarse. ➢ Cuando se trate de solicitudes genéricas que no especifiquen la identidad del interesado o los derechos que desea ejercer.
PROCEDIMIENTO	1º.- Valorar que se cumplen los requisitos de contenido de la solicitud y del derecho. 2º.- Una vez comprobada la solicitud o subsanación se procederá a dar cumplimiento de la petición realizada. **Si los datos están siendo usados por terceros,** se les debe requerir para que procedan a ejercitar el derecho solicitado. En caso de omisión o negativa, AECEMCO lo notificará a la AEPD.
PLAZO	**Se deben responder en el plazo de 1 mes** a partir de la recepción de la solicitud. **Dicho plazo podrá prorrogarse otros dos meses** por la complejidad o el número de solicitudes, previa información al afectado de la prórroga en el plazo de 1 mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. **Si se presenta en oficina de correos**, los plazos empezarán a contar a partir del día siguiente a su recepción en AECEMCO.
DENEGACIÓN	**Se** deberá informar y motivar la negativa, dentro del plazo de un 1 desde su presentación y se informará de su derecho a presentar reclamación ante la AEPD. **La prueba del cumplimiento del deber de responder a la solicitud** de ejercicio de sus derechos formulado por el afectado recaerá sobre AECEMCO, por lo que debe documentarse adecuadamente todo el procedimiento.
REGISTRO	De todas las solicitudes presentadas, con indicación del sentido de la respuesta.

13.- RESUMEN DE LAS MEDIDAS DE SEGURIDAD, A APLICAR DURANTE EL CICLO DE VIDA DE LOS DATOS, RECOGIDAS EN ESTE DOCUMENTO

PROTECCIÓN DESDE EL DISEÑO Y POR DEFECTO

	MEDIDA	RECURSOS	REGISTRO
AECEMCO	**Nombramiento entre el personal de un Responsable** de coordinar y controlar las medidas de aplicación definidas. **Recabar solo los datos necesarios**, exactos, actualizados y por el periodo mínimo imprescindible.	▪ Nombramiento del responsable de Seguridad. • Limitación de perfiles de personal con acceso.	

OBTENCIÓN DE LOS DATOS

COLECTIVO	MEDIDA	RECURSOS	REGISTRO
TRABAJADORES/AS DE AECEMCO	**Recabar consentimiento expreso** para el tratamiento de sus datos personales. **Informar de la existencia** del sistema de video vigilancia.	▪ Consentimiento para el tratamiento de su CV. ▪ Consentimiento para el uso de sus datos personales. ▪ Consentimiento para el uso de fotografías. ▪ Consentimiento para el tratamiento de sus datos biométricos (huella dactilar). ▪ Comunicado la existencia del sistema de video vigilancia.	▪ Registro de Actuaciones de tratamiento. ▪ Inventario de ficheros.

	Compromiso de confidencialidad.	▪ Documento de confidencialidad.	
PROVEEDORES	**Recabar el consentimiento** e Informar del tratamiento de datos.	▪ Cláusula al pie de facturas y formularios. ▪ Pie de página de correo electrónico y transmisiones de fax.	
PERSONAS USUARIAS	**Recabar el consentimiento expreso e Informar** del tratamiento de datos. **Informar del ejercicio de derechos** sobre sus datos personales.	▪ Consentimiento para el uso de sus datos personales. ▪ Consentimiento para el uso de fotografías. ▪ Pie de página de correo electrónico y transmisiones de fax. ▪ Locuciones telefónicas. ▪ Política de privacidad.	

USO

	MEDIDA	RECURSOS	REGISTRO
SENSIBILIZACIÓN Y FORMACIÓN	**Entrega de copia del documento de Seguridad**	▪ Copia del Documento de Seguridad	▪ Registro de recepción del documento de seguridad por parte del personal.
INSTALACIONES	**Control de accesos presencial** en puerta principal. **Sistema de video vigilancia.** **Sala de servidores** bajo llave. **Armarios y ficheros** bajo llave. **Equipos informáticos** protegidos con contraseñas personalizadas y seguras.		▪ Registro de ubicación de ficheros con datos personales.
ACCESO	**Acceso limitado y con autorización.** **Contraseña segura** para el acceso a ficheros automatizados. **Sistema seguro de archivo** y acceso a ficheros no automatizados.		▪ Registro de personal con acceso a datos personales. ▪
TRATAMIENTO	**Entrada, salida y devolución de soportes y ficheros** solo con autorización. **Alta, baja o destrucción de ficheros temporales** sometida a autorización.	▪ Autorización de Entrada, salida y devolución de soportes y ficheros. ▪ Cifrado de datos.	▪ Registro de accesos informáticos. ▪ Inventarios de Hardware y Software.

	Control de accesos informáticos. **Trasmisiones seguras en redes.** **Envíos seguros de ficheros** no automatizados (papel).	▪ Envíos en sobre cerrado y correo certificado.	

DIVULGACIÓN

	MEDIDA	RECURSOS	REGISTRO
TRASFERENCIAS DE DATOS	**AECEMCO no cede datos personales a terceros** salvo en el caso de determinadas externalizaciones de trabajos y servicios y los que precisan las entidades que forman parte de AECEMCO para el desarrollo de programas. **AECEMCO no realiza trasferencias internacionales** de datos.	▪ Contrato con los Encargados del Tratamiento ▪ Adenda a los contratos suscritos con terceros (Añadir a los contratos firmados antes de la entrada en vigor del RGPD)	▪ Relación de empresas externas con acceso a datos personales.

ALMACENAMIENTO, BLOQUEO Y DESTRUCCIÓN

	MEDIDA	RECURSOS	REGISTRO
COPIAS DE RESPALDO Y RECUPERACIÓN	**Realización de copias de seguridad y respaldos.**	▪ Solicitud para la recuperación de datos.	
GESTIÓN DE INCIDENCIAS	**Procedimiento de gestión de incidencias.**	▪ Notificación de incidencias. ▪ Notificación de incidencias a la AEPD y, en su caso al interesado.	▪ Registro de incidencias.
BLOQUEO	**Procedimiento de bloqueo temporal** de los datos personales de un titular a consecuencia del ejercicio de este del derecho de limitación o de eliminación durante el tiempo preciso para cumplir una obligación legal o atender a responsabilidades de un contrato.	▪ Ver apartado *de Derechos de los titulares de datos personales (ejercicio).*	
DESTRUCCIÓN	**Destrucción de ficheros confidenciales** una vez han cumplido su finalidad o ha transcurrido el plazo legal de conservación.	▪ Formulario de destrucción de ficheros.	▪ Baja en el Registro de Actividades de tratamiento y en Inventario de soportes.

DERECHOS DE LOS TITULARES DE DATOS PERSONALES

	MEDIDA	RECURSOS	REGISTRO
INFORMACIÓN	**Informar de los derechos que pueden ejercitar ante AECEMCO** en el mismo momento de recabar el consentimiento expreso.	▪ Ver apartado de *Obtención de Datos* (personas usuarias).	
EJERCICIO	**Procedimiento para el ejercicio** de los derechos.	▪ Formularios para el ejercicio de los derechos	▪ Registro de solicitudes de derechos.
RECLAMACIÓN	**Informar al titular de la posibilidad de reclamación ante la AEPD** en el mismo momento de recabar el consentimiento expreso y en el caso de denegación de la solicitud. **Informar al titular de la posibilidad de reclamar indemnización por**	▪ Ver apartado de *Obtención de Datos* (personas usuarias). ▪ Ver apartado de *Gestión de incidencias* (*notificación de*	

	daños y perjuicios en la comunicación de una brecha de seguridad (incidencia) que afecte a sus datos personales.	*incidencias a la AEPD y al interesado).*	

OTRAS MEDIDAS

	MEDIDA	RECURSOS	REGISTRO
DOCUMENTO DE SEGURIDAD	**Actualización de las Medidas de seguridad.**	▪ Recogida de propuestas de Revisión. ▪ Informe. ▪ Auditorias	Revisiones al Documento de Seguridad.

14.- PLAZOS DE CONSERVACIÓN DE Y SUPRESIÓN DE DATOS PERSONALES

14.1.- Plazos generales

Sus datos personales se tratarán mientras sean necesarios para mantener la relación que los origina.

Con carácter General, estos plazos serán:

Los datos personales de los participantes en premios y concursos serán conservados durante la tramitación del procedimiento de concesión del premio.

Los datos económicos se conservarán al amparo de lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria, y de la normativa de archivos y documentación.

Los datos personales de las personas interesadas en la recepción de información institucional se mantendrán en el sistema de forma indefinida en tanto el interesado no solicite su supresión.

Los datos personales de las personas inscritas en actividades generales serán suprimidos cuando éstas hubieran finalizado.

Los datos personales de las personas inscritas en actividades dirigidas a sectores de actividad o profesionales determinados se mantendrán de forma indefinida en tanto el interesado no solicite su supresión.

Los datos de personal voluntario se conservarán durante 2 años

Los datos del personal laboral se conservarán durante cinco años, salvo que sea preciso un periodo de conservación mayor previsto en la normativa de justificación de una Convenio o Proyecto.

Los datos personales vinculados a la generación de contraseñas de acceso a recursos y sistemas se cancelaran cuando se cancele el acceso al servicio para las que fueron creadas

Los datos personales de las personas que firman en representación de las entidades que suscriben convenios con COCEMFE se mantendrán de forma indefinida. Será de aplicación lo dispuesto en la normativa de archivos y documentación.

Los datos relacionados con el ejercicio de los Derechos de las personas Se conservarán durante el tiempo necesario para resolver las reclamaciones.

Los datos de solicitantes de empleo y de los profesores intervinientes en acciones formativas se conservarán para futuras incorporaciones o acciones formativas, salvo que soliciten su supresión. En el caso de actividades remuneradas se conservarán al amparo de lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria.

Los datos relacionados con la gestión de brechas de seguridad, se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

En todo caso una vez finalizada la acción que legitima el tratamiento, COCEMFE conservará los datos personales convenientemente bloqueados durante el periodo legal necesario para el ejercicio o la defensa frente a acciones administrativas, a disposición exclusiva de jueces y tribunales, Ministerio Fiscal, o las Administraciones Públicas competentes, y por el plazo de prescripción de las mismas. Finalizado este periodo, los datos serán definitivamente cancelados.

14.2. Plazos específicos

Dichos plazos de prescripción pueden ser consultados en el cuadro siguiente:

Ley General de comunicaciones
Se establece un periodo de prescripción de sanciones de: • muy graves a los 3 años • las graves a los 2 años • leves a los 6 meses.
Código de comercio
En una sociedad, existe una serie de documentación que se deberá conservar al menos durante 6 años: • Libro diario • Registro de inventarios y balances • Facturas emitidas • Facturas recibidas
Reglamento de Facturación
Esta normativa enuncia que en el caso de que sea una persona física el emisor o receptor, el período de conservación de la factura será de 5 años a partir de su emisión. Las facturas en las que el emisor o receptor sea persona física, se conservan durante un período de cinco años a partir de su emisión.
Ley general Tributaria
Esta normativa dispone un plazo de 4 años para que se puedan ejercitar derechos, ya sean formales o económicos por parte del contribuyente o la Administración. Los datos relacionados con el IVA y el IRPF se conservarán un mínimo de 4 años
Ley de prevención de blanqueo de capitales
AECEMCO conservará durante un período mínimo de 10 años la documentación en que se formalice el cumplimiento de las obligaciones establecidas en dicha Ley.
Seguridad Social
Queda establecido que para que prescriba la obligación del pago de las cuotas a la Seguridad Social han de pasar 5 años, contar desde la fecha en la que debieron ser ingresadas.
Documentación relativa a los expedientes generados por Departamento Jurídico, abogado o Procurador

Se conservarán al menos durante 5 años los expedientes ya que es el plazo en el cual se podrán ejercitar responsabilidades profesionales.

Ley de Mediación en asuntos civiles o mercantiles

Como es lógico, un procedimiento de mediación puede concluir con acuerdo o no, y sobre el mismo pueden recaer futuras responsabilidades.

Por lo tanto se almacenará al menos durante 4 meses el expediente de la mediación.

Videovigilancia

Las imágenes/sonidos captados por los sistemas de videovigilancia serán canceladas en el plazo máximo de 1 mes desde su captación.

Excepciones

Si de la observación de las grabaciones se aprecian infracciones penales o administrativas graves o muy graves y existe una investigación policial en curso no se podrán eliminar.

Acceso a edificios

1 mes para cancelar los datos incluidos en ficheros automatizados para controlar el acceso a edificios.

Ley de Seguridad privada

Los informes de investigación deberán conservarse archivados, al menos, durante 3 años, incluidas las imágenes grabadas. No obstante lo datos estarán debidamente bloqueados.

Datos de Salud

Como regla general AECEMCO conservará los datos de salud, una vez finalizada la relación jurídica que legitime el tratamiento durante un plazo máximo de 5 años, debidamente bloqueados.

No obstante, en algunas comunidades autónomas, para ciertos casos prevén periodos diferentes de conservación, por lo que AECEMCO podrá ampliar el periodo de 5 años en esos casos especiales:

CA Cantabria. 15 años para la conservación de la historia clínica desde la muerte del paciente.

CA Galicia. Se conservarán de forma indefinida:

- informes de alta
- hojas de consentimiento informado
- hojas de alta voluntaria
- informes quirúrgicos y/o registros de parto
- documentos de anestesia
- informes de exploraciones complementarias. Documentación relativa a necropsias
- hoja de evolución y de planificación de cuidados de enfermería
- otros informes médicos
- cualquier otra información que se considere relevante a efectos asistenciales, preventivos, epidemiológicos o de investigación
- información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales

CA Canarias que regula la historia clínica en los centros y establecimientos hospitalarios. Se conservarán durante 20 años desde la última acción asistencial la siguiente documentación:

- autorización de ingreso
- consentimiento informado
- hoja quirúrgica
- órdenes médicas
- informe de control de medicación
- hojas del recién nacido, de su propia historia clínica
- informes de anestesia
- listas transfusión
- informes de exploraciones complementarias
- solicitud de alta voluntaria
- informes de Anatomía Patológica.
- documentación de necropsias.
- información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales

No obstante, se conservarán de manera definitiva:

- los informes clínicos de alta
- las hojas de anamnesis y exploración física y las hojas de evolución de los episodios asistenciales de los que no exista informe de alta

País Vasco. Se podrá destruir toda la documentación clínica de un paciente una vez transcurridos 10 años desde su fallecimiento.

También se podrá destruir la histórica clínica que haya permanecido sin movimientos durante 15 años.

Reglamento de centros de reconocimiento destinados a verificar las aptitudes psicofísicas de los conductores

El centro conservará durante 10 años el contenido de los informes emitidos, así como los documentos que aportó, en su momento el interesado.

Derecho hotelero

Los libros-registro de entrada en los establecimientos hoteleros deberán almacenarse durante 3 años, a disposición de los Cuerpos y Fuerzas de Seguridad del Estado

Derecho de Internet

Los prestadores de servicios de comunicaciones electrónicas podrán conservar al menos durante 1 año:

- Identificador de usuario
- dirección IP
- número de teléfono
- IMSI e IMEI
- fecha y hora de la comunicación electrónica
- identificación del tipo de servicio utilizado (voz, datos, SMS o MMS)

Subvenciones

La documentación relativa a la justificación de programas y acciones subvencionadas por otros organismos y/o entidades se conservará como mínimo el tiempo exigido para su justificación y/o auditoria o inspección en su respectiva convocatoria.

15.- PROCEDIMIENTO DE REVISIÓN DEL DOCUMENTO DE SEGURIDAD

15.1.- Revisión del documento de seguridad

El Documento de Seguridad de AECEMCO debe mantenerse actualizado y debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados.

En todo caso se entenderá como cambio relevante el que pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

15.2.- Auditorías

Mediante la auditoría se verifica la correcta implantación de las medidas de seguridad a adoptar en la organización,

FASES

AECEMCO se someterá, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de las medidas del Documento de Seguridad.

Con carácter extraordinario se realizará una Auditoria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas. Esta auditoría inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias y estará a disposición de la AEPD.

En el caso de someterse a una AUDITORIA EXTERNA, serán los propios auditores quienes determinen su procedimiento de trabajo.

16.- NORMAS Y PROCEDIMIENTOS DE SEGURIDAD DE AECEMCO

Las medidas de este Documento de Seguridad son de obligado conocimiento y cumplimiento para todo el personal, tanto de AECEMCO como de terceras empresas o entidades, que lleve a cabo cualquier tipo de tratamiento sobre datos de carácter personal.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, podrá ser sancionable conforme a lo previsto en el XV Convenio Colectivo General de Centros y Servicios de Atención a Personas con Discapacidad de aplicación en AECEMCO.

17.- PLAZOS A CUMPLIR Y TIEMPO DE CUSTODIA DE LOS REGISTROS

RESPONSABLE DE SEGURIDAD

ACCIÓN	PLAZO	OBSERVACIONES
NOMBRAMIENTO	CADA 4 AÑOS	RESPONSABLE DEL FICHERO
REVISIÓN	ANUAL	RESPONSABLE DE SEGURIDAD

REGISTRO DE PERSONAL AUTORIZADO CON ACCESO A DATOS PERSONALES

ACCIÓN	PLAZO	OBSERVACIONES
ACTUALIZACIÓN	ANUAL	RESPONSABLE DE SEGURIDAD
REVISIÓN	ANUAL	RESPONSABLE DE SEGURIDAD

REGISTRO DE ACCESOS A FICHEROS AUTOMATIZADOS (INFORMÁTICOS)

ACCIÓN	PLAZO	OBSERVACIONES
INFORME	ANUAL	RESPONSABLE DE SEGURIDAD
REVISIÓN	ANUAL	RESPONSABLE DE SEGURIDAD
CONSERVACIÓN DE LOS DATOS	2 AÑOS	RESPONSABLE DE SEGURIDAD

REGISTRO DE ACCESOS PARA FICHEROS NO AUTOMATIZADOS (PAPEL)

ACCIÓN	PLAZO	OBSERVACIONES
REVISIÓN	ANUAL	RESPONSABLE DE SEGURIDAD
CONSERVACIÓN DE LOS DATOS	2 AÑOS	RESPONSABLE DE SEGURIDAD

REGISTRO DE INCIDENCIAS

ACCIÓN	PLAZO	OBSERVACIONES
REVISIÓN	SEMESTRAL	RESPONSABLE DE SEGURIDAD
ANALISIS	ANUAL	RESPONSABLE DE SEGURIDAD

RESTO DE LOS REGISTROS

ACCIÓN	PLAZO	OBSERVACIONES
REVISIÓN	ANUAL	RESPONSABLE DE SEGURIDAD

CONTRASEÑAS

ACCIÓN	PLAZO	OBSERVACIONES
MODIFICACIÓN	ANUAL	DEPARTAMENTO DE INFORMÁTICA

COPIAS DE RESPALDO

ACCIÓN	PLAZO	OBSERVACIONES
COPIA DE SEGURIDAD DE LOS ARCHIVOS AUTOMATIZADOS DEL SERVIDOR	SEMANAL	DEPARTAMENTO DE INFORMÁTICA
COPIA ANUAL	ANUAL	DEPARTAMENTO DE INFORMATICA
CONSERVACIÓN DE COPIAS ANUALES	5 AÑOS	RESPONSABLE DE SEGURIDAD

FICHEROS CONFIDENCIALES

ACCIÓN	PLAZO	OBSERVACIONES
INFORME SOBRE SU DESTRUCCIÓN	ANUAL	RESPONSABLE DE SEGURIDAD

DERECHOS DE LOS USUARIOS

ACCIÓN	PLAZO	OBSERVACIONES
SUBSANACIÓN DE LA SOLICITUD	15 DIAS	
RESOLUCIÓN DE LA SOLICITUD	1 MES	2 MESES, PREVIA COMUNICACIÓN DENTRO DEL PRIMER MES

AUDITORIA

ACCIÓN	PLAZO	OBSERVACIONES
REALIZACIÓN	CADA DOS AÑOS	INTERNA (RESPONSABLE DE SEGURIDAD) O EXTERNA
COMPROBACIÓN DE MEDIDAS ADOPTADAS	3 MESES POSTERIORES A LA AUDITORIA	RESPONSABLE DE SEGURIDAD

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

ACCIÓN	PLAZO	OBSERVACIONES
REVISIÓN	CUANDO SE PRODUZCAN CAMBIOS RELEVANTES	RESPONSABLE DE SEGURIDAD

18.- DEFINICIONES INCLUIDAS EN ESTE DOCUMENTO

Para la correcta implantación de las medidas de carácter técnico y organizativo contenidas en el Documento de Seguridad, resulta necesario incluir las definiciones que nos da la normativa sobre los términos usados.

Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Fichero: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Perfil de usuario: accesos autorizados a un grupo de usuarios.

Recurso: cualquier parte componente de un sistema de información.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

19.-ANEXOS AL DOCUMENTO DE SEGURIDAD

Los Anexos del Documento de Seguridad, se contemplan los registros y formularios que documentan las medidas de seguridad implantadas y la adecuación de AECEMCO a lo previsto en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos digitales (LOPD), y su normativa de desarrollo.

Dichos anexos están disponibles para la AEPD pero no figuran en la versión del mismo entregada a las personas trabajadoras ya que algunos de ellos quedan también bajo la esfera de protección prevista en el propio Documento de Seguridad, al contener datos personales cuyo conocimiento no precisa la totalidad del personal contratado por AECEMCO para el desarrollo de sus funciones.

Los anexos serán los que a continuación se especifican y se ajustaran a los formatos que aquí se establecen:

Anexo I.- Aprobación del documento de Seguridad

Este anexo recogerá el documento que certifique la aprobación del presente Documento de Seguridad, con indicación:

Anexo II.- Actividades de Tratamiento de Datos Personales

Este Anexo recogerá todas y cada una de las actividades de Tratamiento que realiza AECEMCO y que deberán estar a disposición de los titulares de los datos personales.

Cada una de ellas se registrará en una ficha individualizada que deberá ajustarse al siguiente formato:

Nº DE TRATAMIENTO Y NOMBRE DEL MISMO
Finalidades
Legitimación
Cesiones o comunicaciones
Transferencia Internacional de datos
Procedencia
Tiempo de conservación de los datos

Anexo III - Registros

1.- Registro de Actuaciones de Tratamiento (Descripción de ficheros)

Este registro contiene una relación de los ficheros que contienen datos personales que utilizan las personas contratadas por COCEMFE. Se ajustará al siguiente formato y se adjuntan tantas hojas como fueran necesario

Nº.- Numeración del Tratamiento al que pertenece
NOMBRE: Nombre del tratamiento (Fichero)
F. ALTA: fecha de inicio del tratamiento
F. BAJA: fecha de fin del tratamiento
PROTECCIÓN: Se consignará B en caso de protección baja y A en caso de protección alta (datos personales de carácter sensibles)

Nº	NOMBRE FICHERO	F. ALTA	INFORMAT	PROTECCION	F. BAJA

2.- Registro de Ubicación de ficheros

Este registro contiene una relación de la ubicación de los ficheros que contienen datos personales que utilizan las personas contratadas por COCEMFE. Se ajustará al siguiente formato y se adjuntan tantas hojas como fueran necesario

Nº.- Numeración del Tratamiento al que pertenece
NOMBRE: Nombre del tratamiento (Fichero)
AUTOMATIZADO: Consignar SI en caso de Ficheros ubicados en soportes informáticos; NO en caso de ficheros en formato papel. AMBOS, si se utilizan los dos formatos
UBICACIÓN: Se consignará RUTA en caso de ficheros automatizados; Nº de Armario y Balda en caso de ficheros no automatizados

Nº	NOMBRE FICHERO	AUTOM.	UBICACIÓN

3.- Registro de Autorizaciones

Este Registro contiene una relación de las personas con acceso autorizado a cada uno de los ficheros

TIPO- Carácter de la autorización. Consignar P en cao de autorizaciones de carácter permanente. Consignar EX en caso de autorizaciones de carácter excepcional
UBICACIÓN: lugar dónde se ubica el trabajador (si no es en la central poner sólo la provincia)
FECHA DE ALTA: fecha de inicio de la autorización
FUNCIÓN: es el trabajo a realizar con el fichero – ej. Intermediación laboral
F. BAJA: fecha de fin de la autorización

TIPO	NOMBRE FICHERO	UBICACIÓN	DNI	F. ALTA	FUNCIÓN	F. BAJA

4.- Relación de contratos con empresas Externas

Este Registro contiene la relación de las empresas externas con acceso autorizado a cada uno de los ficheros

FECHA DE ACCESO A LOS DATOS: Fecha de inicio de la autorización

EMPRESA: Denominación social
CIF: Número de identificación fiscal
PERSONA RESPONSABLE: Datos de Contacto del Delegado de protección de Datos, en su caso, o del Responsable de Seguridad
FICHEROS: Número y denominación de los Tratamientos (ficheros) a los que accede
FECHA DE DEVOLUCIÓN DE FICHEROS: Fecha de Fin de la autorización de Acceso.
MECANISMO DE ACCESO: Indicar si se autoriza el acceso y/o cesión mediante Adenda as un contrato o inclusión de cláusulas en el mismo (ADD) o mediante la firma de un contrato de Encargado de Tratamiento (E)
TRABAJO A REALIZAR: trabajo para el que se autoriza el Acceso

FECHA DE ACCESO A LOS DATOS	EMPRESA	CIF	PERSONA RESPONSABLE	TRABAJO A REALIZAR	FICHEROS	MECANISMO DE ACCESO	FECHA DE DEVOLUCIÓN DE FICHEROS

5.-Registro de software empleado en el tratamiento de los ficheros de carácter personal

Este Registro contiene la relación del Software empleado en el tratamiento de datos personales

NOMBRE	LICENCIAS	DESCRIPCIÓN

6.- Registro de hardware empleado en el tratamiento de los ficheros de carácter personal

Este Registro contiene la relación de los Hardware (dispositivos) empleado en el tratamiento de datos personales

TIPO	DESCRIPCION	CARACTERISTICAS	UBICACION

7.- Registro de Incidencias

Este Registro contiene la relación de incidencias que puedan originar una brecha de seguridad en relación con los datos personales.

Nº REGISTRO: referencia numérica de control de la incidencia
FECHA DEL INCIDENTE: Fecha en la que se produce el incidente
FECHA DE NOTIFICACIÓN: Fecha en la que se notifica al Responsable de Seguridad la incidencia producida
INCIDENCIA: descripción del suceso acontecido
MEDIDA APLICADA: Medida de seguridad aplicada o, en su caso medida alternativa
COMUNICACIÓN A LA AEPD: consignar SI/NO y, en su caso, fecha de la comunicación.
COMUNICACIÓN A LOS AFECTADOS: consignar SI/NO y, en su caso, fecha de la comunicación.

Nº REGISTRO	FECHA DEL INCIDENTE	FECHA DE NOTIFICACIÓN	FICHEROS AFECTADOS	INCIDENCIA	MEDIDA APLICADA	COMIUNICACIÓN A LA AEPD	COMUNCIACIÓN A LOS AFECTADOS

8.- Registro de solicitudes de ejercicio de derechos por parte de los usuarios

Este Registro Contiene la relación de solicitudes de ejercicios de derechos recibidas en relación con los tratamientos de los mismos efectuados.

Nº REGISTRO: referencia numérica de control de la incidencia
FECHA DE ENTRADA: Fecha en la que se produce la recepción de la solicitud
OBJETO: descripción de la acción solicitada por el titular del derecho
DOCUMENTOS QUE SE ADJUNTAN: descripción de los documentos que se adjuntan para sustentar la solicitud
ACCIÓN REALIZADA: acción realizada por AECEMCO en relación con la solicitud sustanciada
FECHA DE NOTIFICACIÓN: consignar fecha de notificación a los aceptados de la acción realizada.

Nº REGISTRO	FECHA ENTRADA	OBJETO DE LA SOLICITUD	DOCUMENTOS QUE SE ADJUNTAN	ACCION REALIZADA	FECHA NOTIFICACIÓN

Anexo IV.- Nombramiento del Responsable de Seguridad

Este anexo recogerá el nombramiento del Responsable de Seguridad, dónde debe constar:

- Datos de identificación del órgano que lo nombra
- Datos de la persona nominada y aceptación por ésta del nombramiento
- Duración del nombramiento
- Funciones
- Ficheros para los que se emite el nombramiento

Anexo V.- Formularios

En este Anexo se recogerán los modelos de formularios de uso más frecuente numerados del 1 al 15:

Anexo VI.- Revisiones al Documento de Seguridad

Este anexo recogerá las sucesivas revisiones a las que fuera sometido el presente documento de seguridad y deberá ajustarse al siguiente formato e incluir, en su caso copia de la nueva versión del mismo señalando el número de orden que le corresponda dentro de

las Versiones ya establecidas, las observaciones al mismo, en su caso, y la fecha prevista de la próxima revisión, ajustándose al siguiente formato:

Fecha

Revisado por:	Departamento Jurídico	
	Departamento de Informática	
	Fecha 1ª Versión:	Nº Total de Paginas:
	Fecha de esta revisión:	Nº Total de Paginas:
Órgano que aprueba este documento		Fecha de aprobación:

Observaciones

Fecha de la próxima revisión


AECEMCO
ASOCIACIÓN EMPRESARIAL DE
CENTROS ESPECIALES DE EMPLEO