# Descripción de las actividades de tratamiento realizadas como Responsable del Tratamiento

**Nombre del Responsable:** FUNDACION ASTURIANA DE LA ENERGIA
**CIF:** G74000878
**Domicilio:** C/ FRAY PAULINO ALVAREZ, S/N, C.P. 33600, de MIERES.
**Teléfono:** 985467180
**Correo electrónico:** faen@faen.es
**Delegado de protección de datos:** PRODAT PRINCIPADO, S.L. - TORRECERREDO, 4 - BAJO - 33012 OVIEDO - 985 11 40 57 - DPDASTURIAS@PRODAT.ES

| | **LABORAL** |
|---|---|
| **TRATAMIENTO** | Tratamiento de datos personales de los trabajadores de la Fundación, necesarios para la celebración del contrato, gestión de nóminas, prevención de riesgos laborales y demás obligaciones establecidas en la legislación laboral y de Seguridad Social. |
| **Interesados** | Empleados<br>Solicitantes |
| **Finalidades** | Recursos humanos<br>Prevención de Riesgos Laborales<br>Gestión de nóminas<br>Formación<br>Promoción<br>Registro horario<br>Gestión de actividad sindical |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales<br>Art. 6.1 b) RGPD: El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales<br>Art. 6.1 c) RGPD: El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al Responsable del Tratamiento<br><br>· Real Decreto Legislativo 2/2015 de 23 de octubre por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores |
| **Categorías de datos personales** | Datos identificativos: nombre y apellidos, NIF, dirección, n.º seguridad social, firma manual, imagen y teléfono<br>Características personales: fecha y lugar de nacimiento, edad, sexo, nacionalidad<br>Datos académicos y profesionales: formación, titulaciones, experiencia profesional<br>Datos económicos y financieros: cuentas bancarias, retenciones, datos económicos de nómina<br>Datos especiales: datos de salud (bajas por enfermedad y accidentes laborales, sin inclusión de diagnósticos). En su caso, afiliación sindical, a los exclusivos |

| | |
|---|---|
| | efectos de pagos de cuotas sindicales<br>Datos de detalles de empleo: control de presencia y registro de jornada |
| **Destinatarios de la información** | Entidad a quien se encomiende la prevención de riesgos laborales<br>Tesorería General de la Seguridad Social<br>Servicios autonómicos y estatales Públicos de Empleo<br>En su caso, organizaciones sindicales<br>Entidades financieras<br>Entidades aseguradoras<br>Agencia Estatal de la Administración Tributaria<br>Auditores contables |
| **Plazos de supresión** | En general, los datos personales se mantendrán mientras dure la relación laboral con la entidad y durante el plazo de prescripción de las acciones que pudieran derivarse de conformidad con la normativa laboral, de Seguridad Social o administrativa.<br><br>Los currículums recibidos por diferentes vías se mantendrán durante el plazo de un año desde la recepción. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| **TRATAMIENTO** | **BECARIOS**<br><br>Tratamiento de datos personales de los becarios que realizan sus prácticas en la entidad |
|---|---|
| **Interesados** | Estudiantes y becarios |
| **Finalidades** | Formación<br>Prevención de riesgos laborales |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales<br>Art. 6.1 b) RGPD: El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales |

| | |
|---|---|
| **Categorías de datos personales** | Datos identificativos: nombre y apellidos, NIF, dirección, n.º seguridad social, firma manual, imagen<br>Características personales: fecha de nacimiento, edad, sexo, nacionalidad<br>Datos académicos y profesionales: formación, titulaciones, experiencia profesional |
| **Destinatarios de la información** | Entidades ofertantes de los programas de becas<br>Entidad a quien se encomiende la prevención de riesgos laborales<br>Entidades aseguradoras |
| **Plazos de supresión** | En general, los datos personales se mantendrán mientras dure la relación laboral con la entidad y durante el plazo de prescripción de las acciones que pudieran derivarse de conformidad con la normativa laboral, de Seguridad Social o administrativa.<br><br>Los currículums recibidos por diferentes vías se mantendrán durante el plazo de un año desde la recepción. |
| **Descripción general de medidas técnicas y organizativas de seguridad:** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| **TRATAMIENTO** | **SOCIOS**<br>Tratamiento de datos personales de los socios de la fundación |
|---|---|
| **Interesados** | Socios y miembros |
| **Finalidades** | Gestión de socios y miembros de fundaciones<br>Gestión y organización de actividades fundacionales<br>Comunicación electrónica |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales<br>Art. 6.1 b) RGPD: El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales |
| **Categorías de datos personales** | Datos identificativos: nombre y apellidos, NIF, dirección, n.º seguridad social, firma manual, imagen |

| | |
|---|---|
| **Destinatarios de la información** | Administración Tributaria<br>Entidades bancarias |
| **Plazos de supresión** | Los datos del socio o colaborador se mantendrán mientras dure la relación con la Fundación y mientras se encuentren vigente los plazos de prescripción de las diferentes acciones que pudiesen corresponden a las partes.<br><br>En particular, los datos económicos se mantendrán de conformidad con la Ley 58/2003 General Tributaria.<br><br>Los datos relativos a los interesados en la recepción de comunicaciones electrónicas se mantendrán en los sistemas de la Fundación de forma indefinida mientras la persona interesada no solicite la oposición. |
| **Descripción general de medidas técnicas y organizativas de seguridad:** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| | |
|---|---|
| | **PROVEEDORES - COLABORADORES** |
| **TRATAMIENTO** | Tratamiento de datos personales de los proveedores, acreedores y colaboradores necesarios para mantener la relación comercial y/o contractual con los mismos. |
| **Interesados** | Proveedores |
| **Finalidades** | Gestión contable, fiscal y administrativa |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales<br>Art. 6.1 b) RGPD: El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales |
| **Categorías de datos personales objeto de tratamiento** | Datos identificativos: nombre y apellidos, NIF, dirección, firma manual<br>Datos económicos y financieros: cuentas bancarias |
| **Destinatarios de la información** | Administración Tributaria<br>Entidades bancarias |
| **Plazos de supresión** | Los datos del colaborador se mantendrán mientras dure la relación con la Fundación y mientras se encuentren vigente los plazos de prescripción de las diferentes acciones que pudiesen corresponden a las partes.<br><br>En particular, los datos económicos se mantendrán de conformidad con la Ley |

| | |
|---|---|
| | 58/2003 General Tributaria. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| | |
|---|---|
| | **CONTABILIDAD - GESTIÓN FISCAL** |
| **TRATAMIENTO** | Tratamiento de datos personales necesarios para la llevanza de la facturación, contabilidad y gestión fiscal de la entidad |
| **Interesados** | Socios<br>Proveedores, acreedores y colaboradores<br>Personal laboral |
| **Fines del tratamiento** | Gestión de clientes, contable, fiscal y administrativa |
| **Bases legitimadoras** | Art. 6.1 c) RGPD: El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al Responsable del Tratamiento<br>• Ley 49/2002 de 23 de diciembre de Régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales del mecenazgo<br>• Ley 22/2015 de 20 de julio de Auditoría de Cuentas y Real Decreto 1517/2011 |
| **Categorías de datos personales** | Datos identificativos: nombre y apellidos, NIF, dirección, firma manual<br>Datos económicos y financieros: cuentas bancarias y datos económicos de nómina |
| **Destinatarios de la información** | Agencia Estatal de la Administración Tributaria<br>Entidades financieras<br>Auditores contables |
| **Plazos de supresión** | Los datos personales se mantendrán mientras dure la relación con la Fundación y mientras se encuentren vigente los plazos de prescripción de las diferentes acciones que pudiesen corresponden a las partes.<br><br>En particular, los datos económicos se mantendrán de conformidad con la Ley 58/2003 General Tributaria. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| | |
|---|---|
| | **ADMINISTRACIÓN INTERNA** |
| **TRATAMIENTO** | Tratamiento de datos personales necesarios para la gestión y administración interna de la Fundación, así como de los datos personales relacionados con los órganos de representación de la Fundación y el Patronato |
| **Interesados** | Socios<br>Miembros del Patronato y miembros de representación<br>Personal laboral |
| **Finalidades** | Gestión de clientes, contable, fiscal y administrativa |
| **Bases legitimadoras** | Art. 6.1 c) RGPD: El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al Responsable del Tratamiento<br>• Ley 50/2002 de Fundaciones<br>• Ley 49/2002 de 23 de diciembre de Régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales del mecenazgo<br>• Ley 19/2013 de 9 de diciembre de transparencia, acceso a la información pública y buen gobierno<br>• Ley 22/2015 de 20 de julio de Auditoría de Cuentas y Real Decreto 1517/2011 |
| **Categorías de datos personales** | Datos identificativos: nombre y apellidos, NIF, dirección, firma manual<br>Datos económicos y financieros: cuentas bancarias |
| **Destinatarios** | Agencia Estatal de la Administración Tributaria<br>Entidades financieras |
| **Plazos de supresión** | Los datos personales se mantendrán mientras dure la relación con la Fundación y mientras se encuentren vigente los plazos de prescripción de las diferentes acciones que pudiesen corresponden a las partes.<br><br>En particular, los datos económicos se mantendrán de conformidad con la Ley 58/2003 General Tributaria. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |
| | **JORNADAS Y EVENTOS** |
| **TRATAMIENTO** | Tratamiento de datos personales necesarios para la organización y gestión de eventos y jornadas, así como para el envío de comunicaciones electrónicas |

| | |
|---|---|
| | relacionadas con los mismos. |
| **Interesados** | Solicitantes |
| **Finalidades** | Gestión de actividades culturales, asociativas o deportivas<br>Comunicación electrónica |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales<br>Art. 6.1 b) RGPD: El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales |
| **Categorías de datos personales objeto de tratamiento** | Datos identificativos: nombre y apellidos, NIF, dirección, firma manual, imagen |
| **Plazos de supresión** | Los datos personales se conservarán durante la organización del evento o jornada y, posteriormente, siempre que exista una obligación legal de conservación.<br><br>Los datos relativos a los interesados en la recepción de comunicaciones electrónicas se mantendrán en los sistemas de la Fundación de forma indefinida mientras la persona interesada no solicite la oposición. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |
| **TRATAMIENTO** | **PUBLICACIONES**<br>Tratamiento de imágenes y vídeos publicados en la web y demás redes sociales de la entidad |
| **Interesados** | Socios<br>Asistentes a eventos y jornadas<br>Empleados<br>Becarios |
| **Finalidades** | Gestión de actividades asociativas, culturales o deportivas<br>Promoción |
| **Bases legitimadoras** | Art. 6.1 a) RGPD: El interesado ha dado su consentimiento para el tratamiento de sus datos personales |

| | |
|---|---|
| **Categorías de datos objeto del tratamiento** | Datos identificativos: nombre y apellidos e imagen |
| **Destinatarios y transferencias internacionales de datos** | Está prevista la realización de transferencias internacionales de datos a entidades amparadas en el Escudo de Privacidad EEUU – UE, como consecuencia de la publicación de imágenes en redes sociales norteamericanas |
| **Plazos de supresión** | Las imágenes y vídeos se mantendrán en los sistemas de la Fundación en tanto la persona interesada no solicite su supresión |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

| | |
|---|---|
| | **VIDEOVIGILANCIA** |
| **TRATAMIENTO** | Tratamiento de imágenes captadas por el sistema de videovigilancia de la entidad. |
| **Interesados** | Empleados<br>Socios y usuarios<br>Proveedores y colaboradores |
| **Finalidades** | Seguridad y control de acceso a edificios<br>Videovigilancia |
| **Categorías de datos personales** | Datos identificativos: imagen |
| **Destinatarios de la información** | Fuerzas y Cuerpos de Seguridad<br>Órganos judiciales |
| **Plazos de supresión** | Las imágenes se suprimirán a los treinta días de su captación de conformidad con la Orden INT/316/2011 de 1 de febrero. |
| **Descripción general de medidas técnicas y organizativas de seguridad** | El apartado “Medidas de seguridad aplicadas en los tratamientos de este registro” recoge la lista de las medidas de seguridad más relevantes. |

## Descripción de las actividades de tratamiento realizadas como Encargado del Tratamiento

En la actualidad, la FUNDACION ASTURIANA DE LA  ENERGIA no realiza actividades de tratamiento de datos de personas físicas en calidad de Encargado del Tratamiento

# Descripción de las medidas de seguridad aplicadas a los tratamientos de este Registro

## 1. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS DEFINIDAS Y DOCUMENTADAS

Las funciones de los usuarios finales se recogen en el **DOCUMENTO DE MEDIDAS DE SEGURIDAD.**

1. En el Anexo V. Relación de usuarios y perfiles de usuario autorizados donde se establecen las operaciones autorizadas por usuario o perfil.
2. En el Anexo VII. Circular de medidas de seguridad donde se establecen las obligaciones de todos los usuarios en materia de seguridad y confidencialidad.

## 2. TRABAJO FUERA DE LOS LOCALES (O ACCESO REMOTO) SUJETO A AUTORIZACIÓN

Con carácter general, no está permitido el tratamiento de datos de carácter personal fuera de los locales de la entidad, excepto en los casos autorizados. La autorización para realizar trabajos con datos personales fuera de los locales y centros de trabajo de FUNDACIÓN ASTURIANA DE LA ENERGIA puede establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez de la autorización.

### Modalidad de trabajo mediante acceso remoto

Todos los accesos remotos a sistemas de información son autorizados. En todo caso, y salvo autorización previa, está terminantemente prohibido grabar en un sistema externo cualquier dato accedido remotamente.

Los responsables de sistemas de información encargados de configurar y habilitar los accesos remotos garantizan para los accesos remotos un nivel de seguridad equivalente al de los accesos en modo local.

### Modalidad de trabajo mediante dispositivos portátiles

Los usuarios de FUNDACION ASTURIANA DE LA ENERGIA que utilizan equipos portátiles, no pueden almacenar datos de carácter personal en los discos locales de los mismos, salvo que cuenten con autorización para ello.

Estos tratamientos deben aplicar las mismas medidas de seguridad dispuestas en este documento, por tanto es obligatorio que en los dispositivos portátiles se habiliten los criterios establecidos sobre identificación, autenticación y control de accesos definidos en este documento de medidas de seguridad, siempre que se conecten a las redes y sistemas de FUNDACION ASTURIANA DE LA ENERGIA o accedan de manera remota.

***Categorías especiales de datos: no se realizan tratamientos de datos de carácter personal en dispositivos portátiles que no permitan su cifrado, excepto en los casos recogidos motivadamente en el anexo Anexo IV. Inventarios de equipos, soportes y dispositivos de archivo y, en todo caso, se adoptan medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.***

## 3. DESIGNACIÓN DE LAS PERSONAS CON FUNCIONES DE CONTROL DE LA SEGURIDAD

### Funciones de los administradores de seguridad

Son las personas autorizadas para conceder, modificar o anular el acceso de los usuarios a:

- los sistemas de información (redes informáticas, ordenadores y equipos, servidores, aplicaciones, servicios en línea, etc)
- los sistemas de archivo de documentación en soporte papel

Sus funciones también incluyen:

- Implantar las medidas de seguridad recogidas en el documento de medidas de seguridad para aquellos sistemas de información que controlan.

Únicamente conceden el acceso a los usuarios en base a los criterios definidos por FUNDACIÓN ASTURIANA DE LA ENERGÍA en el documento de medidas de seguridad y previa autorización de la dirección

### Identificación de los administradores de seguridad

**El administrador de sistemas, y de documentación en soporte papel esta fehacientemente nombrado en el DOCUMENTO DE MEDIDAS DE SEGURIDAD *Anexo VI. Nombramientos*.**

## 4. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y REGISTRO DE INCIDENTES DE SEGURIDAD

FUNDACION ASTURIANA DE LA ENERGÍA recoge cuantas incidencias de seguridad se produzcan sobre los datos que trata. Este procedimiento establece los mecanismos de actuación por parte de los usuarios de los sistemas de información para la comunicación, gestión y respuesta ante las incidencias. La aplicación del procedimiento se establece para todos los usuarios, tanto empleados como colaboradores externos.

Se interpreta el concepto de incidencia en su sentido más amplio, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan.

El Administrador de sistemas gestiona la implantación del procedimiento de gestión de incidencias, y realiza el seguimiento de todas las incidencias en materia de seguridad.

Todos **los usuarios están fechacientemente informados de la obligación de notificar cualquier incidencia** producida en materia de seguridad.

### Descripción del procedimiento e información a registrar

Los usuarios de los sistemas de información, empleados y colaboradores externos, participan en la implantación y seguimiento del sistema de gestión de incidencias, aceptando formalmente sus obligaciones.

**Comunicación de incidencias de Seguridad por parte de los usuarios**

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia de seguridad, actual o posible, lo comunica con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

Todas las comunicaciones se efectúan al Administrador de Seguridad indicando el momento en que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente. Para que quede constancia de la comunicación, el usuario, además, lo comunica por correo electrónico.

En este momento se registra la incidencia, y si afecta a la seguridad de los datos de carácter personal, se cataloga como tal.

**Registro y distribución de las incidencias**

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis, se centraliza la recepción de las mismas ante el Administrador de Seguridad.

**Contenido del registro de incidencias**

El registro de incidencias se mantiene en exclusiva por el Administrador de Seguridad. Se facilita el acceso estrictamente a aquellos usuarios o áreas que lo necesiten, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

- El registro contiene como mínimo los siguientes campos:

1. Tipo de incidencia
2. Momento en que se ha producido (en su defecto detección)
3. Persona que la notifica
4. Quién la recibe
5. A quién se le notifica
6. Efectos causados por la misma

**Notificación de las violaciones de seguridad a las autoridades y personas afectadas**

El RGPD establece la obligación de realizar las siguientes notificaciones:

Notificación a las autoridades de protección de datos (Agencia Española de Protección de Datos u otra autoridad competente) de aquellas violaciones de seguridad que supongan un riesgo para los derechos y libertades para las personas físicas, conforme al artículo 33 del RGPD. La notificación se hará dentro de las 72 horas después de tener constancia del incidente.

Notificación a las personas físicas cuyos datos se hayan visto comprometidos, de aquellas violaciones de seguridad que supongan un alto riesgo para los derechos y libertades para las personas físicas. La notificación se harán sin dilación indebida, conforme al artículo 34 del RGPD.

Las violaciones se comunican de forma inmediata al delegado de protección de datos

## 5. PROCEDIMIENTO DE GESTIÓN DE SOPORTES INCLUYENDO SU IDENTIFICACIÓN, INVENTARIO, DESECHO DE SOPORTES CON BORRADO IRREVERSIBLE O DESTRUCCIÓN

Definimos **soporte** como aquel 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. Algunos de los soportes más comunes son:

1. Ordenadores, servidores, portátiles, unidades NAS y demás equipos informáticos.

2. Dispositivos de almacenamiento como discos flexibles, cintas, discos ópticos (CD, DVD, etc), tarjetas de memoria, unidades de memoria USB, discos duros externos, etc.
3. Armarios o archivadores donde se almacenan los documentos.

Los soportes y documentos que contengan datos de carácter personal en FUNDACIÓN ASTURIANA DE LA ENERGÍA siempre permiten identificar el tipo de información que contienen, salvo cuando las características físicas del soporte lo imposibiliten.

Todo soporte empleado en FUNDACIÓN ASTURIANA DE LA ENERGÍA para el tratamiento de datos personales debe ser inventariado.

- Dicho inventario se ha incorporado en el DOCUMENTO DE MEDIDAS DE SEGURIDAD como **Anexo IV. Inventarios de equipos, soportes y dispositivos de archivo**

Dicho anexo puede incluir el listado completo o bien una referencia al documento o sistema donde se mantiene actualizado.

Los soportes que contengan datos de carácter personal se almacenan de tal forma que sólo tienen acceso las personas autorizadas, según el régimen de autorización recogido en el DOCUMENTO DE MEDIDAS DE SEGURIDAD como **Anexo V. Relación de usuarios y perfiles de usuario autorizados**.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera d
e los locales de FUNDACIÓN ASTURIANA DE LA ENERGÍA deben ser autorizados por el responsable del tratamiento o encontrarse debidamente autorizada en el documento de medidas de seguridad.

En caso de reutilización de un soporte, se procede a eliminar toda la información almacenada en el mismo mediante el uso de una herramienta específica que impida cualquier recuperación posterior de información.

Cuando vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal (por ejemplo porque presente errores en su tratamiento) debe procederse a su destrucción, de manera que se impida la reconstrucción posterior del documento (por ejemplo mediante el uso de destructora).

## 6. CONTROL DE ACCESO EN BASE A CRITERIO DE MÍNIMO NECESARIO

Los usuarios tienen acceso únicamente a aquellos datos que precisen para el desarrollo de sus funciones. Se encuentran establecidos mecanismos para evitar que un usuario pueda acceder a recursos distintos de los autorizados. Existe una relación actualizada de usuarios, perfiles de usuario y accesos autorizados en el **DOCUMENTO DE MEDIDAS DE SEGURIDAD - Anexo V. Relación de usuarios y perfiles de usuario autorizados**

En dicho anexo también se recoge el personal autorizado para conceder, alterar o anular el acceso a los recursos, siempre conforme a los criterios establecidos por FUNDACIÓN ASTURIANA DE LA ENERGÍA y siguiendo instrucciones de la dirección.

El acceso por parte de otras personas está estrictamente prohibido, y únicamente puede producirse mediante petición firmada del interesado y autorización por escrito de la dirección.

El personal ajeno a FUNDACIÓN ASTURIANA DE LA ENERGÍA con acceso a los locales y recursos ámbito del presente documento de medidas de seguridad está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

## 7. IDENTIFICACIÓN Y AUTENTICACIÓN INEQUÍVOCA DE LOS USUARIOS

Los procedimientos seguidos para la identificación y autenticación de los usuarios cuando intentan acceder a los sistemas, las redes o las aplicaciones están basados en la combinación de un código de identificación de usuario y una contraseña. A cada usuario le han sido asignados identificadores individuales tanto para el acceso a los sistemas, como para el acceso a las aplicaciones (en aquellos casos en los que sea posible).

## 8. RENOVACIÓN PERIÓDICA DE LAS CREDENCIALES DE ACCESO

Únicamente las personas designadas para ello, tienen competencias para autorizar el alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y datos.

Todas las contraseñas deben ser modificadas por el usuario al menos con la frecuencia establecida. En los entornos en los que sea posible se automatiza este requerimiento de caducidad. Cuando no sea posible, el usuario es responsable del cambio sistemático.

En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia de la entidad.

## 9. CIFRADO DE CONTRASEÑAS

Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.

Las contraseñas se almacenan cifradas, y ninguna persona tendrá acceso a la descodificación de las mismas.

En el caso del sistema y la red, las contraseñas se almacenan cifradas por sus propias herramientas de seguridad. En el caso de las aplicaciones, el cifrado de las contraseñas es realizado por el sistema gestor de bases de datos o por un desarrollo "ad hoc" de la propia aplicación.

Las contraseñas de usuarios de emergencia, propios de los sistemas y con máximos privilegios, serán custodiadas por la entidad.

## 10. COPIAS DE SEGURIDAD

El Administrador de Sistemas se encarga de controlar la correcta aplicación de los procedimientos de forma que se cumplan los siguientes requisitos:

- Todos los soportes utilizados para las copias de seguridad cumplen las normas relativas a identificación de los soportes, inventariado y almacenamiento con las **correspondientes medidas de control de acceso** (armario con llave, caja ignífuga, etc) que garanticen que únicamente sean utilizados por el personal encargado de la ejecución de los procedimientos de copia de respaldo.
- Los procedimientos de copia de seguridad **cubren la totalidad de tratamientos automatizados de datos personales** incluidos en servidores, bases de datos, soportes móviles y demás dispositivos.

- La **periodicidad de la copia es al menos semanal**, salvo que en dicho periodo no se hubiera producido ninguna modificación de los datos.
- Los procedimientos para la recuperación de los datos **garantizan su recuperación en el estado en que se encontraban** al tiempo de producirse la pérdida o destrucción.
- Cuando se vayan a realizar pruebas con datos reales, es obligatorio realizar previamente copia de todos los datos afectados.
- Para evitar pérdida de datos en caso de mal funcionamiento de alguno de los soportes de copia, se mantienen varios soportes de copias.