POLÍTICA DE SEGURIDAD del personal + Funciones y obligaciones I+D

POLÍTICA DE SEGURIDAD DEL PERSONAL PARA EL TRATAMIENTO DE DATOS PERSONALES

1.- ÁMBITO DE APLICACIÓN

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la organización, por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que se le ha encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos que tiene que seguir el personal de la organización, tanto propio como externo, que trata datos personales en el desarrollo de su actividad, y se basa en lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

En este sentido, para velar y hacer cumplir esta Política, la organización ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

2.- CONCEPTOS BÁSICOS

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

Estructura del tratamiento:

- **Datos personales**: Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento**: Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado**: Persona física sometida al tratamiento de sus datos personales.
- **Fichero**: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
- **Responsable del tratamiento**: Organización que determina los fines y los medios del tratamiento.
- **Personal autorizado**: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

Categorías de datos:

- **Básicos**: Datos que no correspondan a categorías Penales o Especiales, por ejemplo: nombre, dirección, e-mail, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.
- **Penales**: Datos relativos a la comisión de infracciones administrativas o penales, o datos que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud**: lealtad y transparencia con el interesado.
- **Limitación de los fines**: tratados para fines determinados.
- **Minimización de los datos**: solo se deben obtener los datos necesarios para alcanzar los fines.
- **Exactitud**: actualizados.
- **Limitación del plazo de conservación**: guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad**: aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva**: se debe poder demostrar el cumplimiento de todos los principios de protección de datos.

Consentimiento para realizar un tratamiento de datos

- Cuando el tratamiento de datos personales se base en el consentimiento del interesado, deberemos obtener el consentimiento explícito para tratarlos y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos de que la comunicación sea lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, para emitir una factura), en una relación contractual, o en un interés legítimo, público o vital.

Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación de los datos o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:

    - Los destinatarios o categorías de destinatarios de los datos.
    - La transmisión de datos a países u organizaciones establecidas fuera de la UE.
- Y si los datos no se se han obtenido del interesado:
    - Categoría de datos.
    - Fuentes de procedencia.

Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para conocer qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento**: Organización que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos**: Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.

Medidas de seguridad

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento a consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

4 - FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar en todo momento conforme a las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal está obligado a cumplir expresamente:

Organización de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación, supresión y portabilidad de los datos y limitación u oposición al tratamiento.

Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo conservarse en el lugar apropiado al término de la jornada laboral.

Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, y salvaguardar las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona solo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos que puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

Eliminación de documentos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de

documentos.

Copia de seguridad y recuperación de datos

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la organización.

Protección de datos

Se deberán aplicar las medidas de protección de datos establecidas por la organización relativas a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, *antispam*, etc.

Gestión de incidencias

Se considera una incidencia cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia de la que tenga conocimiento al Responsable de seguridad para su conocimiento y para la aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. La persona que notifica la incidencia deberá documentarla con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligado a atender a consecuencia de dicho incumplimiento.

FUNCIONES Y OBLIGACIONES DE OBLIGADO CUMPLIMIENTO

USUARIOS son todas aquellas personas que ejercen sus funciones bajo la autoridad del RESPONSABLE que intervienen en el tratamiento de cualquier información generada por la organización relativa tanto a datos personales como a los que no lo son. Estos deberán actuar de acuerdo con las instrucciones contempladas en el Acuerdo de confidencialidad y secreto profesional, obligándose además a cumplir las funciones y obligaciones relacionadas en este anexo.

I. Confidencialidad de la información

Están **expresamente prohibidas** las siguientes actividades:

1. Enviar al exterior o revelar a terceros, información que no haya sido declarada como no confidencial

por el RESPONSABLE, mediante cualquier procedimiento o soporte, sea electrónico, digital, manual o documental, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso a la misma.

2. El uso de cámaras fotográficas, de vídeo, de sonido o cualquier instrumento que pueda almacenar información audiovisual, entendida esta no solo de personas, sino de cualquier lugar, soporte o recurso del RESPONSABLE.

3. Divulgar directamente o a través de terceras personas o empresas los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral o profesional con la organización, tanto en soporte material como electrónico. Esta prohibición continuará vigente tras la extinción del contrato laboral por tiempo indefinido.

4. Poseer, para usos fuera de su responsabilidad, ningún material o información propiedad del RESPONSABLE o del cliente del mismo donde se presten los servicios, tanto ahora como en el futuro.

En caso de que, por motivos directamente relacionados con el puesto de trabajo, el USUARIO entre en posesión de información que no haya sido declarada como no confidencial por parte del RESPONSABLE, bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le otorgue derecho alguno de posesión, titularidad o copia sobre la referida información.

Asimismo, el USUARIO deberá devolver dichos materiales al RESPONSABLE inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación laboral o profesional. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento del RESPONSABLE, no supondrá, en ningún caso, una modificación de esta cláusula.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en los artículos 197 y 278 del Código Penal y dará derecho al RESPONSABLE a proceder como estime oportuno en defensa de sus intereses y a exigir al USUARIO una indemnización económica.

II. Utilización de los sistemas informáticos (SI)

El Sistema Informático, y los terminales utilizados por cada USUARIO son, con carácter general, propiedad del RESPONSABLE o de un cliente del mismo.

Están **expresamente prohibidas** las siguientes actividades:

1. El uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial. Su incumplimiento podrá ser causa de responsabilidad disciplinaria, administrativa, civil y penal.

2. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos del RESPONSABLE o de terceros. Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal.

3. Introducir voluntariamente programas, virus, macros, *applets*, controles ActiveX o cualquier otro

dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los Sistemas Informáticos del RESPONSABLE o de terceros. Al respecto, recordar que el propio sistema ejecuta automáticamente los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

4. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por el RESPONSABLE. Esta prohibición incluye cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

5. Instalar copias ilegales de cualquier programa, incluidos los que están estandarizados.

6. Borrar cualquiera de los programas instalados legalmente.

7. Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos del RESPONSABLE.

8. Cifrar información sin estar expresamente autorizado para ello.

III. Salvaguarda y protección de las contraseñas personales

Están **expresamente prohibidas** las siguientes actividades:

1. Compartir o facilitar el identificador de usuario y la clave de acceso (contraseña) proporcionado por el RESPONSABLE a otra persona física o jurídica. Si el USUARIO sospecha que otra persona conoce sus datos de identificación y acceso deberá notificar al Responsable de seguridad de esta incidencia para activar los mecanismos de cambio de contraseña. En caso de incumplimiento de esta prohibición, el USUARIO será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificación.

2. Intentar distorsionar o falsear los registros *log* del sistema.

3. Intentar aumentar o disminuir el nivel de privilegios de un USUARIO en el sistema.

IV. Acceso a redes

Están **expresamente prohibidas** las siguientes actividades:

1. Utilizar los datos, la red corporativa y/o la intranet del RESPONSABLE y/o de terceros para incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la organización y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

2. Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del RESPONSABLE.

3. Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos del RESPONSABLE y/o de terceros.

4. Almacenar datos de carácter personal en el disco duro del ordenador, debiendo ser utilizadas para tal fin las carpetas de la red corporativa asignadas por el RESPONSABLE.

5. Obstaculizar voluntariamente el acceso de otros USUARIOS a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la organización, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

V. Recursos telemáticos y acceso a Internet

El RESPONSABLE se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un USUARIO.

Cualquier fichero introducido en los SI desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, en las referidas a propiedad intelectual y a control de virus.

Están **expresamente prohibidas** las siguientes actividades:

1. Utilizar los recursos telemáticos del RESPONSABLE y/o acceder a redes públicas como Internet, páginas web (www), grupos de noticias (*Newsgroups*) y otras fuentes de información como FTP, etc. para temas no relacionados directamente con la actividad del RESPONSABLE o los cometidos del puesto de trabajo del USUARIO.

2. El acceso a debates en tiempo real (Chat/IRC), ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema.

VI. Utilización del correo electrónico y mensajería

Se considerará correo electrónico tanto el interno como el externo, dirigido o proveniente de otras redes privadas o públicas, especialmente Internet.

Ningún mensaje de correo electrónico será considerado como privado.

El RESPONSABLE se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los USUARIOS de la red corporativa y los archivos *log* del SI, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la organización como responsable civil subsidiario.

Cualquier fichero introducido en los SI a través de mensajes de correo electrónico, provenientes de redes externas, deberá cumplir los requisitos establecidos en estas normas además de las del cliente, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Las direcciones de correo electrónico dirigidas a personas, son consideradas datos personales, por lo que cuando se envíen correos a más de un destinatario, si no es estrictamente necesario que los otros vean las direcciones de correo de todos los demás, se deberán enviar como copia oculta «Cco».

Están **expresamente prohibidas** las siguientes actividades:

1. Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros

USUARIOS. Esta actividad puede constituir un delito de interceptación de las telecomunicaciones (revelación de secretos), previsto en el artículo 197 del Código Penal.

2. Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.

3. Enviar o reenviar mensajes en cadena o de tipo piramidal.

VII. Tratamiento de la información

Están **expresamente prohibidas** las siguientes actividades:

1. Acceder a recursos que no sean necesarios para el desarrollo y cumplimiento de su labor, así como consultar, copiar, reproducir, transmitir, editar, modificar o eliminar información sin estar autorizado para estas funciones.

2. Utilizar impresoras o fotocopiadoras sin recoger de manera inmediata los documentos impresos en la bandeja de salida con el fin de que otras personas no autorizadas puedan acceder a la información.

3. Destruir cualquier documento físico o soporte digital que incluya datos personales sin utilizar la destructora de papel o sin guardarlos debidamente custodiados hasta que sean retirados por una empresa homologada de destrucción de documentos.

4. Dejar la pantalla del ordenador sin bloquear cuando se abandona el puesto de trabajo temporalmente, de modo que no se impida la visualización de la información a personas no autorizadas.

VIII. Gestión de incidencias

Es obligación del USUARIO, comunicar al RESPONSABLE en el menor plazo posible, todas aquellas incidencias que se produzcan en la organización, entendidas estas como cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos personales o al incumplimiento de las obligaciones detalladas en este documento.

Dicha comunicación deberá contener la identificación clara de la incidencia y una descripción detallada de la misma, que contendrá, como mínimo: el momento –día y hora– en que se ha producido, la persona que ha tenido conocimiento de ella, las personas a las que se ha comunicado, los efectos producidos y las medidas correctoras adoptadas.

Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente Anexo al Acuerdo de confidencialidad, por duplicado, en MADRID, a 12/09/2025.

ASOCIACION BARRO,
JUAN DANIEL MOLANO VILLAR

El USUARIO