FUNCIONES Y OBLIGACIONES

COLABORADORES CON ACCESO A DATOS

Por el Árticulo 10 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de Carácter personal (LOPD) se comunica al personal de Avanfi, que las personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional de esos datos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Para poder cumplir con el deber del secreto profesional y el deber de guardar los datos, es necesario respetar las siguientes **obligaciones generales** por parte de cualquier trabajador y/o colaborados de Avanfi.

Las presentes obligaciones generales incluyen a todo el personal, tanto el que desarrolle su labor en dependencias de la empresa, como el que desarrolle su labor en dependencias de terceros.

Identificación de usuarios y claves de acceso.

1. Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá activar los mecanismos de cambio de contraseña.
2. El usuario está obligado a utilizar los datos, la red corporativa y/o la intranet de la Entidad y/o de terceros sin incurrir en Actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la empresa y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.
3. Están **expresamente prohibidas** las siguientes actividades:
    - Compartir o facilitar el identificador de usuario y la clave de acceso facilitado por la Entidad a otra persona física o jurídica. 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 de usuario.
    - Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Entidad.

- 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 árticulo 197 del Código Penal).
- Intentar distorsionar o falsear los registros log del sistema.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Entidad y/o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario del sistema.

Utilización de los sistemas informáticos.

Están **expresamente prohibidas** las siguientes actividades:

1. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Entidad o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del código Penal).
2. El usuario no deberá almacenar datos de carácter personal en el disco duro del ordenador, sino utilizar para tal fin las carpetas de la red corporativa preasignada.
3. 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.
4. Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario
5. Introducir voluntariamente programas, virus, macros, applets, controle 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 de las empresas 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.
6. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la empresa; 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.
7. Instalar copias ilegales de cualquier programa, incluidos los que están estandarizados.
8. Borrar cualquiera de los programas instalados legalmente.
9. Enviar o reenviar mensajes en cadena o de tipo piramidal.

10. Utilizar los recursos telemáticos de la empresa incluida la red Intranet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
11. Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la empresa.
12. Cifrar información sin estar expresamente autorizado para ello.

Confidencialidad de la Información

1. Queda prohibido enviar al exterior información que no haya sido declarada como no confidencial por parte de la empresa, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso a la misma.
2. Los usuarios de los Sistemas de Información corporativos deben guardar por tiempo indefinido la máxima reserva, y no divulgar directamente ni 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 con la Entidad, tanto en soporte material como electrónico. Esta obligación continuará vigente tras extinción del contrato laboral.
3. Ningún colaborador debe poseer, para usos fuera de su responsabilidad, ningún material o información propiedad de la entidad o del cliente de la misma donde se presten los servicios, tanto ahora como en el futuro.
4. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información que no haya sido declarada como **no confidencial** por parte de la empresa, bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia sobre la referida información. Asimismo, el trabajador o colaborador deberá devolver dichos materiales a la Entidad 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. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la Entidad, no supondrá, en ningún caso, una modificación de esta cláusula.

   El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en los artículos 197 y 278 del Código Penal y dará derecho a la Entidad a exigir al usuario una indemnización económica.

Incidencias

1. Es obligación del personal de la Entidad comunicar al responsable de Seguridad de cualquier incidencia que se produzca en los Sistemas de Información a que tengan acceso.
2. Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.
3. Dicha comunicación deberá realizarse en un plazo de tiempo no superior a una hora desde el momento en que se produzca dicha incidencia.

Protección de datos

1. La creación, modificación o supresión de los ficheros que contengan datos de carácter personal deberá notificarse al Responsable de Seguridad y al responsable Funcional del Fichero para que éste lo notifique a la Agencia de Protección de Datos. Asimismo, se notificará cualquier cambio que afecte a la finalidad del fichero, a su responsable o a la ubicación del fichero
   La entidad notificará a los afectados en el momento de recabar los datos:
   - Existencia del fichero
   - Finalidad de la recogida de datos
   - Destinatarios de la información
   - Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
   - Identidad y dirección del responsable del fichero.
   - Consecuencias de no suministrar la información requerida y el carácter obligatorio o no de las respuestas a las preguntas realizadas.
2. La recogida de datos de carácter personal, requerirá el consentimiento expreso y por escrito de los afectados a quienes se les ha solicitado dichos datos, incluida la disponibilidad de los mismos.
3. Se realizarán las cesiones o comunicaciones de datos de carácter personal de acuerdo con los siguientes requisitos:
   - Con consentimiento previo.
   - Cumpliendo fines directamente relacionados con las funciones legítimas de la Entidad y de sus cesionarios.
4. No será necesario recabar el consentimiento de los afectados cuando:
   - La cesión está autorizada por Ley.
   - Se trate de datos recogidos de una fuente accesible al público (repertorios telefónicos, censo promocional, diarios y boletines oficiales, medios de comunicación y listas de Colegios profesionales).
   - El tratamiento responda de una relación jurídica cuyo cumplimiento y control implique la conexión con ficheros de terceros.
5. Se consideran actos prohibidos:

- Crear ficheros de datos personales sin la correspondiente notificación previa al responsable de Seguridad Funcional del Fichero.
- Utilizar los datos personales para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados o para finalidades distintas a las comunicadas, sin la autorización expresa del responsable del fichero.
- Cualquier otra actividad expresamente prohibida en este documento o en ls normas sobre protección de datos e Instrucciones de la Agencia de Protección de datos.

Uso del correo electrónico

1. El sistema informático, y los terminales utilizados por cada usuario son, con carácter general, propiedad de la Entidad o de un cliente de la misma.
2. Ningún mensaje de correo electrónico será considerado como privado. Se considerará correo electrónico tanto el interno, como el externo, dirigido o proveniente de otras redes privadas o públicas, especialmente Internet.
3. La entidad 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 Entidad como responsable civil subsidiario.
4. 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 o además de las del cliente, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Acceso a Internet

1. El uso del sistema informático de la entidad para acceder a redes públicas como internet, se limitará a los temas directamente relacionados con la actividad de la Entidad y los cometidos del puesto de trabajo del usuario.
2. El acceso a debates en tiempo real (Chat/IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.
3. El acceso a páginas web (www), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, se limita a aquellos que contengan información relacionada con la actividad de la Entidad o con los cometidos del puesto de trabajo del usuario.
4. La Entidad 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.
5. Cualquier fichero introducido en los SI desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y a control de virus.

Propiedad Intelectual e industrial

Queda estrictamente prohibido en los sistemas de información que dependan directa o indirectamente de HBMA, 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.

El no cumplimiento de las presentes obligaciones generales podrán ser causa de responsabilidad, disciplinaria, administrativa, civil y penal.

Documentación sanitaria y/o Historias Clínicas

1. En el caso de extracción de documentación sanitaria y/o historias clínicas fuera del archivo asignado por la organización, es obligatorio la anotación correspondiente en el libro de salidas habilitado a tal efecto.
2. En el tiempo que dicha documentación sanitaria este fuera de los archivos asignados, el responsable de su custodia ha de velar por la seguridad de la información, evitando el acceso de personas no autorizadas a dicha información.
3. La devolución de la documentación sanitaria y/o historias clínicas al archivo asignado por la organización se ha de realizar de forma inmediata una vez finalizadas las circunstancias que motivaron su extracción, siguiendo los protocolos establecidos por la organización.
4. Está prohibido la extracción de documentación sanitaria y/o historias clínicas fuera de la entidad sin la autorización expresa de Dirección Médica y en su defecto del Responsable de Seguridad.

Comunicación a terceros

La empresa comunica al colaborador que sus datos personales, entre los que se encuentran la imagen y el sonido de la persona, datos que podrán ser obtenidos mediante sistemas de videovigilancia de cámaras o videocámaras con la única finalidad de salvaguardar la seguridad en el centro, forman parte de uno o varios ficheros de titularidad de HBMA, datos incluidos en la presente relación laboral que podrán ser comunicados a terceros cuando la comunicación responda a cualquiera de las siguientes necesidades: Formación, estudio, desarrollo, implantación y mantenimiento de proyectos, seguridad del centro, cumplimiento de acuerdos comerciales, gestión de recursos humanos corporativos de la entidad y control de la relación laboral siempre que se limiten dichas cesiones a las finalidades enunciadas. Sus datos también podrán ser cedidos a terceras empresas cuando esa cesión venga determinada por acuerdos alcanzados en el marco de la negociación colectiva entre empresa y representantes de los trabajadores como establece en el artículo 11 de la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 15/1999 de 13 de Diciembre, para finalidades propias

del objeto de la entidad, para concursos de proyectos ante entidades públicas y privadas que lo requieran, y empresas de control de absentismo a lo cual el trabajador consiente expresamente. Así mismo, los datos personales también serán cedidos siempre que exista una ley habilitante o una norma que así lo disponga.

Asimismo AVANFI garantiza el ejercicio de los derechos de acceso, rectificación, oposición y cancelación reconocidos por la legislación vigente. Para ejercitar tales derechos el interesado deberá realizar una comunicación a la dirección del responsable del fichero, a los referidos efectos, en la calle Orense 32, 28020 de Madrid.

Muy atentamente,

Fecha:

AVANFI,S.L.

El Colaborador:

D.N.I:

p.p. Responsable del Fichero