INFORMACIÓN CONFIDENCIALIDAD Y MEDIDAS DE SEGURIDAD (ANEXO I, II)

(Personal laboral y estudiantes en prácticas/personas colaboradoras)

ANEXO I: CONFIDENCIALIDAD. (Personal laboral y estudiantes en prácticas/personas colaboradoras)

¿Quién es el responsable del tratamiento de tus datos?

Identidad: Avapace

CIF: G46103727

Dir. Postal: Plaza José Mª Orense, 6 bajo - 46022 – Valencia (VALENCIA)

Teléfono: 963604437

Correo-e: protecciondedatos@avapace.org

Contacto DPD.: Julia Gascón

http://www.avapace.org/protecciondatos.php

¿Con qué finalidad tratamos sus datos personales?

En la entidad vamos a tratar sus datos personales con la finalidad de gestionar y mantener la relación interna existente entre la empresa y empleados, y para las siguientes finalidades (Atender a cada caso concreto):

Gestión de la relación laboral y del expediente del trabajador.

Realizar todos aquellos trámites administrativos, fiscales y contables necesarios para cumplir con nuestros compromisos contractuales, obligaciones en materia de normativa laboral, Seguridad Social, prevención de riesgos laborales, fiscal y contable.

Gestión de pago de nóminas mediante entidad financiera.

Cobro de la cuota obrera y traslado de la misma al Sindicato.

Control horario a través del sistema de control de acceso mediante huella/tarjeta.

Control laboral a través de sistemas de videovigilancia.

Control Laboral monitorizando la actividad del usuario en el correo electrónico profesional pudiendo inclusive acceder al contenido de los mismos, control de la actividad llevada a cabo en los equipos y dispositivos tanto físicos como móviles, accediendo a archivos, mensajería instantánea, navegación en Internet, instalación de programas de monitorización de la actividad del usuario.

En su caso, control laboral mediante aplicaciones instaladas en el vehículo (localizador GPS).

Gestión de los seguros colectivos / plan de pensiones de la empresa.

Realizar actuaciones formativas tanto de formación bonificada como no bonificada.

Realizar acciones de patrocinio y publicidad del Responsable que pueden consistir en la publicación de imágenes del empleado en un directorio en la página web o de imágenes sobre la actividad de la empresa en la que aparezcan empleados en la página web de la empresa y sus redes sociales:

Twitter: La red social al ser norteamericana puede transferir datos a Estados Unidos por lo que le recomendamos conocer su política de privacidad: http://www.twitterenespanol.net/privacy_policy.php

Facebook: La red social al ser norteamericana puede transferir datos a Estados Unidos por lo que le recomendamos conocer su política de privacidad: https://es-es.facebook.com/privacy/explanation

Instagram: La red social al ser norteamericana puede transferir datos a Estados Unidos por lo que le recomendamos conocer su política de privacidad: https://es-la.facebook.com/help/instagram/155833707900388

Whatsapp: La red social al ser norteamericana puede transferir datos a Estados Unidos por lo que le recomendamos conocer su política de privacidad: https://www.whatsapp.com/legal/?lg=es&lc=ES&eea=1

YouTube: La red social al ser norteamericana puede transferir datos a Estados Unidos por lo que le recomendamos conocer su política de privacidad: https://www.youtube.com/yt/policyandsafety/es/policy.html

Asimismo, le informamos de que las instalaciones de la entidad disponen de un sistema de videovigilancia permanente por razones de seguridad, y en caso de ser necesario para control laboral.

¿Durante cuánto tiempo vamos a conservar sus datos personales?

• Sus datos personales serán conservados mientras dure la relación laboral con la entidad.

Al finalizar la misma, los datos personales tratados en cada una de las finalidades indicadas se mantendrán durante los plazos legalmente previstos o durante el plazo que un juez o tribunal los pueda requerir atendiendo al plazo de prescripción de acciones judiciales. Los datos tratados en base al consentimiento del interesado se mantendrán en tanto no expiren los plazos legales aludidos anteriormente, si hubiera obligación legal de mantenimiento, o de no existir ese plazo legal, hasta que el interesado solicite su supresión o revoque el consentimiento otorgado.

- Las imágenes/sonidos captados por los sistemas de videovigilancia se conservarán durante el plazo máximo de un mes desde su captación, de acuerdo con la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- La información captada mediante sistemas de geolocalización serán guardados durante el plazo de 1 año.
- Las imágenes publicadas en las redes sociales y página web de la entidad se conservarán salvo que solicite la supresión de las mismas.

¿Cuál es la legitimación para el tratamiento de sus datos?

- Ejecución de contrato: La base legal para el tratamiento de sus datos es la ejecución de su contrato laboral.
- Cumplimiento de una obligación legal:
- Los tratamientos de datos derivados las relaciones laborales, están legitimados por el 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.
- Obligación de protección en materia de Prevención de Riesgos Laborales, en virtud de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales.
- Suministro de información a las entidades gestoras de las prestaciones económicas de la Seguridad Social de conformidad con la Ley General de la Seguridad Social.
- Comunicación de sus datos cuando así lo solicite la Inspección de Trabajo. Ley 42/1997, de 14 noviembre, reguladora de la Inspección de Trabajo.
- Obligaciones tributarias de la entidad, conforme a la Ley General Tributaria.

Consentimiento del interesado:

- Publicación de su nombre e imagen y otras informaciones, relacionadas con la actividad de la entidad en redes sociales y página web.
- Descuento de la cuota obrera.

¿A qué destinatarios se comunicarán sus datos?

Sus datos serán comunicados a las entidades y organismos que se detallan a continuación:

- A las entidades bancarias que corresponda, para estar al corriente de pagos.
- A la Administración tributaria.
- Organismos de la Seguridad Social, Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social.

- En el supuesto de que nos sea solicitado, sus datos serán cedidos a la Inspección de Trabajo.
- A las entidades que participen en la gestión de cursos de formación a los que desee asistir el trabajador con la finalidad de participar en los cursos que se organicen. En el caso de recibir formación subvencionada, según establece la Ley orgánica 5/2002 de 19 de junio, de las Cualificaciones y de la Formación Profesional, así como en caso de contratos para la formación y el aprendizaje previstos por el R.D. 1529/2012, deberá facilitarse a las Administraciones públicas competentes, toda la información requerida para el seguimiento y control de las acciones formativas realizadas.
- Al Sindicato al que se encuentra afiliado para el descuento de la cuota obrera.
- En el caso de utilizar vehículos de empresa (incluyendo renting o alquiler), sus datos podrán ser comunicados a las autoridades que en su caso lo requieran, y en todo caso, para la identificación del conductor en caso de infracción de tráfico. También podrán ser comunicados, en su caso, a la compañía de alquiler/renting de vehículos.
- Empresas contratantes siempre que sea imprescindible en cumplimiento de normativa de contratación vigente; en caso de recibir subvenciones dentro de la documentación que se deba proporcionar dentro de las condiciones de la subvención; así como por la participación de Avapace en un concurso o licitación, bien sea directamente o bien a través de la constitución de una Unión Temporal de Empresas (UTE) o incluso en el marco de una futura subcontratación.

Sus datos, en determinados casos, serán comunicados al resto de entidades que forman parte del grupo de empresas.

En el supuesto de que nos haya dado su consentimiento para el tratamiento de su nombre e imágenes y otras informaciones, relacionadas con la actividad de la entidad, se divulgarán en las diferentes redes sociales y página web de la entidad.

Transferencias internacionales.

La entidad no tiene previsto realizar transferencias internacionales de datos, es caso de ser necesarias, sólo se realizarán a entidades bajo la habilitación del acuerdo EEUU-Unión Europea Privacy Shield (más información: https://www.privacyshield.gov/welcome), a entidades que hayan demostrado que cumplen con el nivel de protección y garantías de acuerdo con los parámetros y exigencias previstas en la normativa vigente en materia de protección de datos, como el Reglamento Europeo, o cuando exista un habilitación legal para realizar la transferencia internacional.

Al trabajar en un sistema de carpetas compartidas en la aplicación Dropbox Google Drive, se realizará una transferencia internacional a Estados Unidos bajo la habilitación del acuerdo EEUU-Unión Europea Privacy Shield. Más información: https://www.privacyshield.gov/welcome

¿Cuáles son sus derechos en relación con el tratamiento de datos?

Usted como titular de datos tiene derecho a obtener confirmación sobre la existencia de un tratamiento de sus datos, a acceder a sus datos personales, solicitar la rectificación de los datos que sean inexactos o, en su caso, solicitar la supresión, cuando entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos o usted como interesado retire el consentimiento otorgado.

En determinados supuestos el interesado podrá solicitar la limitación del tratamiento de sus datos, en cuyo caso sólo los conservaremos de acuerdo con la normativa vigente.

En ciertos supuestos podrá ejercitar su derecho a la portabilidad de los datos, que serán entregados en un formato estructurado, de uso común o lectura mecánica a usted o al nuevo responsable de tratamiento que designe.

Tendrá derecho a revocar en cualquier momento el consentimiento para cualquiera de los tratamientos para los que lo ha otorgado.

Disponemos de formularios para el ejercicio de todos los derechos anteriormente indicados, no obstante, también puede utilizar los elaborados por la Agencia Española de Protección de Datos. Estos formularios deberán ir firmados electrónicamente o ser acompañados de fotocopia del DNI. Si se actúa por medio de representante de la misma manera deberá ir acompañado de copia de su DNI o con firma electrónica.

Los formularios deberán ser presentados presencialmente en la entidad o remitidos por correo postal o electrónico en las direcciones que aparecen en el apartado “Responsable”.

Tendrá derecho a presentar una reclamación ante la Agencia Española de Protección de Datos en el supuesto de que considere que no se ha atendido convenientemente el ejercicio de sus derechos.

El plazo máximo para resolver será el de un mes a contar desde la recepción de su solicitud.

En el caso de producirse alguna modificación de sus datos, le agradecemos nos lo comunique debidamente por escrito con la finalidad de mantener sus datos actualizados.

Mediante el presente documento, Avapace cumple su deber de informar a todo el personal sobre las normas de seguridad y protección de datos de carácter personal.

Estas normas son de obligado cumplimiento para todos los miembros de Avapace: personas en plantilla, estudiantes en prácticas, personal externo, colaboradores, etc.

Avapace conservará una copia de este documento firmada por todo el personal.

Confidencialidad y deber de secreto

Todo el personal, en el marco de la relación laboral o de la prestación de servicios que le une con Avapace, se compromete a:

1. No revelar a ninguna persona ajena a Avapace sin el consentimiento de la misma, la información referente a la que haya tenido acceso durante el desempeño de sus funciones en la entidad, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o de la entidad impuestas por leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

2. Utilizar la información que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en Avapace y no disponer de ella de ninguna otra forma o con otra finalidad.

3. No utilizar de ninguna forma cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado o colaborador y que no fuera necesaria para el desempeño de sus funciones en Avapace.

4. Cumplir, en el desarrollo de sus funciones en la entidad Avapace, la normativa vigente, relativa a la protección de datos de carácter personal y, en particular, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

5. Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral o de prestación de servicios que le une con Avapace.

El usuario será responsable, ante Avapace frente a terceros de cualquier daño que pudiera derivarse para unos u otros, del incumplimiento de los compromisos anteriores y resarcirá a la entidad de las indemnizaciones, sanciones o reclamaciones que la entidad se viera obligada a satisfacer como consecuencia de dicho incumplimiento.

En caso de ser Delegado Sindical o miembro del Comité de Avapace, le informamos que el Estatuto de los Trabajadores, establece un deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la entidad o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado. En todo caso, tal y como establece el Estatuto de los Trabajadores, ningún tipo de documento entregado por Avapace al comité podrá ser utilizado fuera del estricto ámbito de la misma ni para fines distintos de los que motivaron su entrega. El deber de secreto sustituirá incluso tras expirado su mandato e independientemente del lugar en que se encuentre.

Asimismo, con la firma de este documento, comprensible sobre las normas de confidencialidad y deber del secreto, así como la información relativa al tratamiento de los datos del personal, alumno en prácticas y colaboradores de Avapace, el trabajador, alumno en prácticas o colaborador declara que lo ha leído y comprendido en toda su extensión.

ANEXO II MEDIDAS DE SEGURIDAD Y PROHIBICIONES (Personal laboral y estudiantes en prácticas/personas colaboradoras)

Las siguientes medidas de seguridad son de obligado cumplimiento para todo el personal de Avapace en relación con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE) en cuyo artículo 32 se dispone que:

- El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros
- El responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo detectado teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.
- Las sanciones por incumplimiento de las estipulaciones del Reglamento pueden acarrear la imposición de sanciones de hasta 20 millones euros o el 4% de la facturación bruta mundial.

A continuación, se presenta un resumen de las medidas de seguridad más relevantes. Esta normativa de seguridad es de obligado cumplimiento para todos los usuarios de Avapace (personal interno y externo, así como estudiantes en prácticas o colaboradores) con acceso a los datos automatizados de carácter personal y a los sistemas de información.

1. En relación a los datos personales almacenados en **soporte papel y cualquier otro dispositivo no electrónico**, se tendrán en cuenta las siguientes normas:

- Cuando la documentación con datos de carácter personal no se encuentre archivada en los dispositivos habilitados para su almacenamiento, por encontrarse en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pudiera ser accedida por personal no autorizado.
- La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado.
- Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, por ejemplo, mediante triturado.
- Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto del traslado.

2. En relación a las **contraseñas** se seguirán las siguientes normas:

- Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares o de amigos y derivados del nombre de usuario como serían mutaciones en cambios de orden o repeticiones de las letras.
- No se accederá al sistema utilizando el identificador y contraseña de otro usuario puesto que es personal e intransferible. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado ya que está prohibido revelar la contraseña a otros usuarios.

3. En relación a los **ordenadores de sobremesa y portátiles** se seguirán las siguientes normas:

- En el caso de tratar datos personales en el dispositivo, se tiene la obligación de trabajar sobre la unidad lógica definida en el servidor central. Se prohíbe almacenar en estos soportes datos personales sin autorización.
- El trabajador que desee utilizar su dispositivo personal, para fines empresariales, deberá comunicarlo previamente a su superior. En caso de autorizarse, el trabajador deberá implementar las medidas de seguridad oportunas que garanticen la seguridad y confidencialidad de sus datos, así como firmar los documentos oportunos.
- El dispositivo es para fines estrictamente laborales y por tanto no se utilizará para fines particulares. Se monitorizará su buen uso controlando los correos electrónicos y su contenido, contenido de mensajería instantánea, uso y navegación de Internet, actividad del usuario mediante herramientas de monitorización de actividad, software de trazabilidad de documentos.
- El usuario que quiera instalar nuevas aplicaciones, ha de solicitar autorización previa escrita al administrador del sistema, así como seguir las instrucciones de descarga, instalación y configuración de seguridad y privacidad.
- El usuario extremará la precaución en el acceso a páginas web en la descarga de ficheros para impedir la entrada de malware que pueda comprometer el funcionamiento del dispositivo.

4. Las siguientes normas se aplicarán a los **soportes de almacenamiento** (PenDrive, CD's, etc) utilizados por los usuarios:

- Se prohíbe almacenar en estos soportes datos personales sin autorización previa del superior.
- El contenido de los soportes podrá ser revisado en cualquier momento.
- En el caso de salida de algún soporte fuera de los locales de la entidad Avapace (salida que deberá ser debidamente autorizada) el usuario adoptará medidas de seguridad dirigidas a evitar la sustracción, posible pérdida o accesos indebidos a la información, la cual en todo caso se mantendrá en dicho soporte cifrada.
- En el momento del desecho de algún soporte, el usuario procederá a su previo borrado o a su destrucción para evitar el acceso o recuperación posterior de la información contenida en el mismo.

5. Respecto al uso de terminales **móviles corporativos** (incluyendo teléfonos, tablets y PDA's):

- el dispositivo es para fines estrictamente laborales y por tanto no se utilizará para fines particulares. Se monitorizará su buen uso controlando el contenido de los correos electrónicos, mensajería instantánea y uso y navegación por Internet.
- el usuario custodiará el dispositivo impidiendo el acceso o manipulación por parte de otras personas.
- es obligatorio hacer servir el bloqueo por código o cualquier mecanismo de protección equivalente disponible en el dispositivo.
- el usuario se abstendrá de desactivar cualquier mecanismo de seguridad que haya estado habilitado por Avapace en el dispositivo, así como el sistema de bloqueo, el sistema de borrado remoto, el cifrado de datos o cualquier otro.
- queda totalmente prohibido el jailbreak o cualquier modificación o re-configuración del dispositivo sin autorización previa escrita del administrador del sistema.
- el usuario que quiera instalar nuevas aplicaciones al dispositivo, ha de solicitar autorización previa escrita al administrador del sistema, así como seguir las instrucciones de descarga, instalación y configuración de seguridad y privacidad.
- en caso de avería o mal funcionamiento del dispositivo se debe notificar inmediatamente al administrador del sistema. También se notificarán pérdidas o robos del dispositivo a fin de proceder a la denuncia, bloqueo y/o borrado remoto.
- está prohibido almacenar o mantener datos personales catalogados como categorías especiales de datos origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona

física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física así como los relativos a condenas e infracciones penales, salvo que se cuente con autorización previa y por escrito de la Dirección.

- el usuario extremará la precaución en el acceso a páginas web en la descarga de ficheros para impedir la entrada de malware que pueda comprometer el funcionamiento del dispositivo.
- en la fecha prevista de devolución o como límite de tiempo la fecha de baja del usuario en Avapace, el usuario devolverá el dispositivo al administrador del sistema para garantizar que se proceda al borrado de la información.
- El uso personal de las comunicaciones telefónicas estará permitido si es fortuito o insignificante, y no interfiere con las actividades laborales habituales ni perjudica el rendimiento de las mismas. El acceso de los usuarios y sus privilegios asociados se verán limitados exclusivamente a aquellos que resulten imprescindibles para desarrollar las funciones correspondientes a sus obligaciones profesionales para con Avapace. Los equipos telefónicos fijos y móviles, así como el fax son propiedad de Avapace, y por tanto, se reserva el derecho de revisar la lista de llamadas realizadas y faxes enviados, para la verificación del cumplimiento de las normas ante cualquier sospecha fundada o evidencia de uso fraudulento o abusivo del servicio.
- el trabajador que desee utilizar su dispositivo móvil personal, para fines empresariales, deberá comunicarlo previamente a su superior. En caso de autorizarse, el trabajador deberá implementar las medidas de seguridad oportunas que garanticen la seguridad y confidencialidad de sus datos, así como firmar los documentos oportunos.

6. En relación a la realización de **pruebas de software**, está prohibido incorporar datos de carácter personal reales en los entornos de desarrollo que no cuenten con las debidas medidas de seguridad y hayan sido autorizados para ello por el administrador del sistema. En dichos entornos desprotegidos se emplearán exclusivamente datos ficticios.

7. Cualquier soporte informático recibido en la organización, deberá ser registrado e inventariado, siguiendo el procedimiento establecido internamente. Una vez procesado, el soporte recibido deberá ser borrado completamente. En el caso de que por un motivo justificado se desee conservar el soporte recibido, deberá inventariarse, siguiendo las normas internas.

8. Respecto al uso de Internet y de la cuenta de correo electrónico facilitada por Avapace, esta será de uso y desarrollo exclusivamente de las funciones laborales del empleado. No podrá utilizarse la cuenta de correo electrónico proporcionada por Avapace para otros fines y se podrá acceder al contenido de los correos electrónicos y comprobar el historial de navegación en Internet.

Avapace, en virtud del artículo 20.3 del Estatuto de los Trabajadores, le informa que “podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana”.

El uso particular queda completamente excluido. No se permite el envío ni recepción de mensajes privados, ni almacenamiento de fotografías ni documentos particulares. Entre los sistemas de control previstos se encuentra el registro y revisión de la navegación, alertas automáticas sobre el envío de mensajes con adjuntos y la revisión de los correos electrónicos sospechosos, así como el acceso a los mismos durante la ausencia del usuario en caso que sea necesario.

Respecto a la **cuenta de correo** asignada por Avapace, se observarán las siguientes normas:

- El usuario mantendrá la contraseña de acceso de manera confidencial y sin facilitarla a otras personas.
- No utilizar una contraseña fácilmente deducible.
- El usuario bloqueará el acceso a la cuenta de correo, en caso de ausentarse del puesto de trabajo durante la jornada.

- En caso de recibir mensajes sospechosos es necesario comunicarlo al administrador del sistema. Ejemplos de mensajes sospechosos son los recibidos por desconocidos, los que simulan el envío desde entidades bancarias o desde Avapaces muy conocidas induciendo a abrir links o soliciten páginas donde se pidan contraseñas o datos personales.
- En caso de detectar una incidencia durante el uso del correo electrónico, la persona trabajadora lo tiene que poner en conocimiento del administrador del sistema.
- Cuando el correo contenga datos de categorías especiales (que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física y relativos a condenas e infracciones penal) no podrá reenviarlo sin autorización de su superior inmediato y deberá en cualquier caso cifrar su contenido y facilitar la contraseña por otra vía.

Solamente podrán utilizar cuentas de webmail corporativas, aquellos empleados que estén autorizados para ello. En este caso, deberán seguirse las siguientes normas en caso de consultar desde un equipo o dispositivo que no pertenezca a Avapace:

- No hacer uso de la opción de guardar la contraseña.
- Al finalizar, cerrar la sesión de webmail y borrar el historial de navegación.
- No deberá guardar datos en terminales o soportes ajenos a Avapace, salvo que fuese estrictamente necesario y procediendo después a su total eliminación.
- Únicamente se consultará el webmail desde ordenadores o dispositivos protegidos mediante contraseña u otro mecanismo de bloqueo.

9. La **salida de soportes informáticos y ordenadores personales** que contengan datos de carácter personal fuera de los locales de Avapace precisa de autorización, que deberá solicitarse al administrador del sistema.

10. Toda **incidencia y brecha** en materia de seguridad deberá comunicarse, siguiendo las instrucciones determinadas en el citado manual, al administrador del sistema tan pronto como se tenga constancia de la misma.

11. Todos los **ficheros temporales** que los usuarios mantengan en sus ordenadores personales deberán ser borrados, una vez haya finalizado la finalidad para la que fueron creados.

12. Queda terminantemente **prohibido iniciar nuevos tratamientos de datos** sin previa autorización de la Dirección.

13. **No está permitido instalar "motu propio"** ningún producto informático o APP en ordenadores, smartphones, tablets y sistemas de información de la organización. Todas aquellas aplicaciones necesarias para el desempeño de su trabajo serán autorizadas por el administrador del sistema e instaladas por personal autorizado para ello. También está prohibido alterar o modificar "motu propio" la configuración del sistema, dispositivo y aplicativos de gestión.

14. Queda prohibido utilizar los recursos de los sistemas a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales de Avapace.

15. Queda terminantemente prohibido facilitar a persona alguna ajena a Avapace ningún soporte conteniendo datos, a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

16. Cualquier solicitud de ejercicio de derechos por parte de un interesado en relación con el tratamiento de sus datos será trasladada inmediatamente a la persona o departamento responsable de estudiarla y responderla.

17. Está absolutamente prohibido almacenar en dispositivos datos personales catalogados como categorías especiales de datos origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física así como los relativos a condenas e infracciones penales, salvo que se cuente con la autorización por escrito de Avapace.

18. Queda prohibido el uso de aplicaciones en la nube para compartir documentos o trabajar fuera del lugar de trabajo, que no estén previamente autorizadas por el administrador del sistema. Algunas de estas aplicaciones del tipo Drive o Dropbox pueden ocasionar una transferencia internacional de datos fuera de la Unión Europea y del Espacio

Económico Europeo, lo que requiere adaptar con carácter previo por parte de Avapace de una serie de medidas y cautelas impuestas por la normativa.

19. En relación con el Delegado de protección de datos / coordinador de protección de datos, el empleado deberá:

- atender a sus requerimientos de información
- facilitarle a la mayor brevedad posible cuanta información hubiera solicitado
- informarle con carácter previo sobre nuevos tratamientos que se vayan a realizar
- informarle con carácter previo sobre cambios organizativos o técnicos en la organización que puedan variar los análisis de riesgos en protección de datos realizados.
- informarle sobre nuevos prestadores de servicios que accedan a datos
- informarle sobre brechas e incidentes de seguridad tan pronto como se tenga constancia de la misma
- informarle sobre la recepción de solicitudes de ejercicio de derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- informarle sobre las transferencias internacionales que se puedan o se piensen realizar

Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral o de prestación de servicios con Avapace

Asimismo, se recuerda que el usuario será responsable frente a Avapace y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a Avapace las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

En el caso de producirse algún cambio en sus datos, rogamos nos lo comunique debidamente por escrito.

Asimismo, con la firma de este documento, comprensible sobre las medidas de seguridad en materia de protección de datos, así como la información relativa al tratamiento de los datos del personal y colaboradores de Avapace, el trabajador o colaborador declara que lo ha leído y comprendido en toda su extensión.