

CONTROL DE VERSIONES

EDICIÓN	FECHA DE REVISIÓN	REVISADO POR	OBSERVACIONES	FECHA DE APROBACIÓN	APROBADO POR
01	03/04/2024	Pablo Tur	Creación del documento	05/04/2024	Responsable de la Información

1. INTRODUCCIÓN

Mediante el presente documento TWIM pone en conocimiento de sus empleados y colaboradores externos, en adelante “**usuarios**”, las normas de obligado cumplimiento que afectan al uso de los recursos y componentes de los Sistemas de Información, en adelante “**SI**”, automatizados y no automatizados (papel), así como a la información y datos de carácter personal que en estos se almacenan y que son objeto de tratamiento.

Todo usuario del SI de TWIM está obligado a la lectura y aceptación de las normas aquí establecidas y se compromete a su cumplimiento.

Funciones y obligaciones de los usuarios: Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información, estarán claramente definidas y documentadas en las políticas y procesos que forman parte del SI.

2. DEFINICIONES

- **Ficheros temporales:** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Responsable del Sistema:** persona asignada formalmente a la función de coordinar y controlar las medidas de seguridad aplicables.
- **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
- **BYOD (bring your own device):** dispositivos personales autorizados por TWIM para su uso.

3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Los contratos firmados entre TWIM y sus clientes establecen cláusulas relativas a la confidencialidad de la información. Los empleados y colaboradores externos de TWIM y sus proveedores que sean usuarios de los sistemas de información de TWIM han de ser conocedores de las citadas cláusulas, siendo deber de TWIM informar de las mismas. Además de las cláusulas específicas de cada contrato, todo usuario debe cumplir el Acuerdo de Confidencialidad que TWIM tiene con sus clientes. Los usuarios tienen el deber de proteger la información a la que tengan acceso como consecuencia de las tareas encomendadas por TWIM.

Una vez finalizada la relación contractual con TWIM, los usuarios se comprometen a no utilizar la información o conocimiento obtenido durante la relación contractual en beneficio propio o de terceras entidades. Además, toda información propiedad de TWIM o de sus clientes debe ser devuelta o destruida.

4. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD E INCIDENCIA CON DATOS PERSONALES

El usuario está obligado a notificar por email cualquier incidente de seguridad o incidencia con datos personales, comunicándose directamente y de forma inminente al Responsable del Sistema para su correcta gestión a la siguiente dirección de correo electrónico [alerta.seguridad@twim.es].

5. NORMAS DE USO DE LOS INDICADORES DE USUARIO Y CONTRASEÑAS

Cada usuario será responsable único de mantener la confidencialidad de sus identificadores de usuario y de sus contraseñas, por lo que se prohíbe la comunicación de los mismos a terceras personas. En caso de incumplimiento de esta prohibición el usuario será el único responsable de los actos realizados por aquellos que los utilicen de forma no autorizada.

Queda prohibido cambiar las contraseñas asignadas a cada usuario para el desarrollo de sus funciones dentro de la Organización (estaciones de trabajo, dispositivos móviles, etc.), las cuales solo se modificarán por el Responsable del Sistema. Para la gestión de las contraseñas se cuenta con el documento **PO-06 · POLÍTICA DE GESTIÓN DE CONTRASEÑAS.docx**.

6. NORMAS DE USO DE LOS EQUIPOS INFORMÁTICOS EN PROPIEDAD

Los equipos de los puestos de trabajo, siempre que por cualquier motivo se abandonen, deben bloquearse para evitar que terceros puedan acceder a los recursos y aplicaciones a las que el usuario legítimo está autorizado (bloqueo automático).

Queda prohibido alterar la configuración de los equipos informáticos y conectar elementos externos (dispositivos móviles, módems, memorias USB, etc.) sin contar con la autorización previa del Responsable del Sistema.

Queda prohibido la utilización de soportes de almacenamiento de información distintos a los instalados y configurados por TWIM para tales fines tales como CD, DVD, memorias USB o de cualquier otro tipo.

Queda prohibido modificar la contraseña de inicio de sesión en las estaciones de trabajo y/o portátiles sin previa autorización y conocimiento del Responsable del Sistema.

Para los equipos informáticos portátiles se deberán adoptar todas las precauciones para evitar su pérdida o sustracción y en caso de que esta se produjese deberá notificarse inmediatamente al Responsable del Sistema para adoptar las medidas de seguridad oportunas.

En caso de que el usuario prevea que no va a utilizar su equipo portátil durante un período prolongado de tiempo deberá depositarlo en las dependencias de TWIM.

El uso de los equipos de prueba, si se necesita, debe ser con previa comunicación y autorización del Responsable del Sistema.

7. INSTALACIÓN DE APLICACIONES Y ALMACENAMIENTO DE CONTENIDOS

Queda prohibido el uso de aplicaciones, así como el almacenamiento de contenidos no afines con las actividades de TWIM. La utilización de programas informáticos sin la debida autorización puede ser constitutiva de responsabilidades de distinto orden, e incurrir asimismo en algún tipo de responsabilidad legal o penal.

Los programas informáticos destinados a ser instalados o efectivamente instalados en los equipos informáticos, así como los contenidos almacenados en los mismos son propiedad de TWIM o de otros terceros legítimos titulares que le han cedido la propiedad o licencia de uso a TWIM. Únicamente el personal designado por el Responsable del Sistema podrá instalar y configurar, o en su caso autorizar a ello, las aplicaciones y software homologados y autorizados por TWIM.

Todos los equipos informáticos de TWIM tienen instalado el programa antivirus corporativo, el cual no se podrá modificar o desactivar. No obstante, el usuario deberá tener la máxima diligencia a la hora de ejecutar archivos procedentes de fuentes no conocidas. En caso de duda, el usuario deberá abstenerse de ejecutar el archivo o programa y contactar directamente con el Responsable del Sistema.

La copia de seguridad se realiza según el documento **PO-08 · POLÍTICA DE COPIAS DE SEGURIDAD.docx**. En el caso de que se produzca una pérdida fortuita o accidental de esos datos quizás nunca puedan recuperarse. Por tanto, es obligatorio almacenar en los servidores habilitados toda la información corporativa.

8. SEGURIDAD FÍSICA Y POLÍTICA DE MESAS LIMPIAS

El acceso físico a las instalaciones de TWIM queda restringido a personal externo a la misma, salvo personal con autorización previa de la Dirección, respetando en todo momento los controles de acceso de seguridad establecidos.

Al finalizar la jornada, los ordenadores deben quedar apagados. En el caso de que sea necesario que permanezcan encendidos, la pantalla debe estar bloqueada. Además, se debe verificar que el material y la documentación utilizada en el desempeño de sus funciones se encuentran debidamente recogidos.

Los papeles para desechar deben destruirse en la destructora de documentos existente en la sede de TWIM.

9. NORMAS DE USO DE DISPOSITIVOS MÓVILES

- Los recursos móviles facilitados o autorizados por TWIM son:
 - Dispositivos facilitados por la TWIM
 - Dispositivos de personal autorizado (BYOD)

Todos los dispositivos estarán bajo el control de las políticas de seguridad de la información establecidas.

El usuario queda obligado en todo caso a dar un uso razonable y equilibrado de éstos en todo momento.

- Queda prohibida la conexión de cualquier tipo de dispositivo móvil de almacenamiento propiedad del usuario a los ordenadores personales y servidores de TWIM.
- Los recursos móviles puestos a disposición de los usuarios de TWIM están sujetos a:
 - La facultad de TWIM de gestionar o administrar sus líneas móviles en razón de las necesidades del trabajo.
 - La titularidad de TWIM sobre los números asignados a los recursos móviles.
 - La política de predeterminación de llamadas salientes para comunicaciones con terceros (clientes y/o proveedores) preseleccionados.
- El usuario que disponga de un recurso móvil de TWIM será depositario y responsable del uso y custodia segura del mismo desde el momento en que se le entrega, garantizando:
 - El uso del mismo solo con fines laborales como norma general.
 - La comunicación inmediata a TWIM en caso de extravío o sustracción del dispositivo
 - En caso de sustracción o extravío del dispositivo, el usuario deberá comunicar directamente al operador de telecomunicaciones correspondiente para que se restrinja la línea inmediatamente y a TWIM en cuanto sea posible.
- El usuario será el único y total responsable del contenido íntegro de los mensajes que envíe a través de su teléfono móvil, así como de los datos que facilite a terceros.
- Los usuarios de recursos móviles habilitados para acceder a Internet y correo electrónico estarán sujetos a las correspondientes normas de acceso y uso de estos servicios con carácter general en TWIM.

- En el caso de servicios de mensajería móvil (SMS/MMS/PUSH) o cualquier tipo de mensajería instantánea, queda prohibida la creación, el almacenamiento o intercambio de contenidos que violen las leyes de derechos de autor y derechos de copia.

También se cuenta con el documento **PO-04 · POLÍTICA TRAE TU PROPIO DISPOSITIVO (BYOD).docx**.

10. NORMAS DE USO DEL CORREO ELECTRÓNICO

- El uso del servicio de correo electrónico siempre debe ser relacionado con actividades afines a la función que se desempeñe dentro de TWIM, de conformidad con las normas vigentes y las reglas del presente documento, teniendo en cuenta que los usuarios que lo utilicen están actuando en su propio nombre, así como en el nombre y en representación de TWIM.
- Queda prohibido modificar la configuración fija del cliente de correo electrónico implementada por el Responsable del Sistema.
- En caso de recibir un mensaje de correo electrónico destinado a otra persona el usuario lo notificará al remitente y acto seguido lo borrará. Ello se aplicará únicamente a aquellos remitentes considerados como fiables.
- Queda prohibido el envío de mensajes a varios destinatarios en lista abierta (campo Para:) salvo que por razones de organización y gestión del trabajo sea preciso.
- Si un usuario recibiera en su correo electrónico mensajes con contenido inadecuado deberá poner esta circunstancia en conocimiento de su superior o comunicarlo directamente al Responsable del Sistema.
- Queda prohibido intercambiar secretos comerciales u otra información confidencial propiedad de TWIM fuera de los casos expresamente autorizados por razón del cargo y desarrollo del trabajo.
- El correo electrónico no podrá ser utilizado para enviar ni para contestar mensajes o cadenas de mensajes. Tampoco podrá ser utilizado con fines comerciales ni lucrativos en beneficio del usuario.
- Se prohíbe expresamente la interceptación, acceso y uso no autorizado de buzones, mensajes o direcciones de correo electrónico de otros usuarios sin la autorización de estos.
- Si un usuario va a estar ausente de su puesto de trabajo por vacaciones, bajas, excedencias, días voluntarios o por cualquier otra causa deberá notificarlo al Responsable del Sistema para generar la debida auto respuesta y su posible redirección del correo a otro usuario por razones de organización.
- Queda prohibido configurar el acceso a cuentas de correo electrónico personales no corporativas en el cliente de correo.
- El usuario debe eliminar todo correo cuya conservación en el tiempo no sea absolutamente imprescindible. Esta norma afecta tanto a los correos recibidos como a los enviados.
- Para evitar cualquier sospecha de entrada de un virus informático u otra amenaza, el usuario cumplirá con la siguiente normativa y deberá informar inmediatamente al Responsable del Sistema:
 - o No ejecutar jamás un ejecutable adjunto a un correo electrónico.

- o No abrir jamás los mensajes de correo provenientes de fuentes desconocidas.
- Queda prohibida la suscripción a listas de correo, revistas, diarios, blogs, chats, publicaciones, grupos de noticias u otros servicios similares. Sólo serán admisibles si están directamente relacionadas con las actividades de TWIM y previa autorización del Responsable del Sistema.

También se cuenta con el documento **PO-07 · POLÍTICA DE USO DE CORREO ELECTRÓNICO.docx**.

11. NORMAS DE USO DE INTERNET

- Queda prohibido modificar la configuración fija del navegador de Internet implementada por el Responsable del Sistema. Esto incluye direcciones IP y DNS, cuya configuración no podrá ser manipulada en ningún caso salvo petición justificada.
- Queda prohibido utilizar los servicios y contenidos de Internet de forma contraria a las condiciones generales de uso que regulen el uso de cada página web.
- Queda prohibido el uso de Internet como vía de acceso para la comisión de acciones ilícitas o contrarias a la legislación vigente, la moral, las buenas costumbres y el orden público.
- El acceso y uso de Internet no podrá ser utilizado con fines comerciales o lucrativos en beneficio propio del usuario.
- Únicamente podrá utilizarse los servicios de Internet para fines particulares o personales cuando dicho uso garantice el cumplimiento de la normativa vigente, siga las normas reflejadas en este documento y las siguientes reglas:
 - Uso ocasional, razonable, racional y moderado en el marco de lo establecido en el presente documento y sin incurrir en los usos prohibidos.
 - No interfiera con la productividad, con la resolución de las tareas diarias y con las responsabilidades asignadas.
 - No dañe la reputación de TWIM.
 - No afecta al rendimiento del sistema de información de TWIM.

12. NORMAS PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El usuario queda informado de toda la reglamentación RGPD de TWIM. El usuario queda obligado al cumplimiento de las normas establecidas por TWIM y RGPD en el tratamiento de datos personales.

- El secreto profesional respecto de los datos personales conocidos, cualquiera que fuere el soporte de tratamiento, nunca se podrá romper, aún después de terminada la relación con TWIM.
- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
- No se desechará documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción efectiva.
- Cada puesto de trabajo es responsabilidad de su usuario autorizado y por ello, tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al mismo deberán estar físicamente ubicados en lugares que garanticen su confidencialidad y restricción de acceso al personal autorizado.
- Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos impresos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Las siguientes actuaciones están prohibidas, las cuales solo pueden ser con previa autorización (**Registro de Autorizaciones**) al Responsable del Sistema:

- Facilitar el acceso de terceras personas a información, incluyendo ficheros automatizados y no automatizados, tanto a nivel lógico como físico.
- Trasladar soportes o documentos con datos personales fuera de las dependencias de TWIM.
- Enviar información contenida en los ficheros de datos a través de ningún tipo de sistema de transmisión de información.
- Realizar cualquier tipo de copia de los ficheros a los que el usuario tiene acceso, en cualquier tipo de soporte.
- Acceder e intentar acceder a datos y recursos no autorizados.
- Utilizar fuera de las instalaciones de TWIM algún soporte de almacenamiento externo que se ha utilizado para almacenar datos personales.
- Ejecutar procedimientos de recuperación de datos.

13. MONITORIZACIÓN Y CONTROL DEL USO DE LAS HERRAMIENTAS DEL USUARIO

TWIM tiene derecho a vigilar, controlar y monitorizar que las herramientas e instrumentos de trabajo (automatizadas o no) sean utilizadas con arreglo a lo dispuesto en este documento, así como en otras normas de TWIM y demás legislación vigente aplicable. Por tanto, el usuario es consciente de que no existen expectativas de intimidad, confidencialidad y secreto de las comunicaciones o actuaciones que se realicen empleando las herramientas e instrumentos de trabajo puestos a su disposición por TWIM, ni aun cuando estos sean tecnológicos.

TWIM podrá acceder, controlar y monitorizar todos los medios tecnológicos puestos a disposición del usuario y en particular, sin carácter limitativo, el uso de internet y el correo electrónico, siempre de conformidad con la ley aplicable y con respeto a los principios de proporcionalidad, racionalidad e idoneidad, con objeto de:

- Comprobar el cumplimiento de lo previsto en este documento y demás normativa vigente aplicable.
- En el caso de las relaciones establecidas entre el usuario y TWIM, vigilar, controlar y verificar el cumplimiento por el usuario de sus obligaciones y deberes de acuerdo con lo establecido en el artículo 20.3 del Estatuto de los Trabajadores, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.
- Toma de acciones legales o reclamar al usuario que incurra en conductas prohibidas, conforme a lo establecido en las normas y leyes vigentes aplicables, y poder demostrar ante los órganos judiciales u otras autoridades tales conductas.

14. INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DEL USUARIO

De acuerdo con la RGPD, TWIM informa al usuario que sus datos de carácter personal derivados de la aplicación de esta normativa serán almacenados con la finalidad de gestionar y dar cumplimiento a las finalidades descritas en el presente documento.

En supuestos excepcionales derivados de necesidades o intereses debidamente acreditados (tal como cuando existan sospechas fundadas de que el comportamiento del usuario perjudica gravemente los intereses empresariales de TWIM y/o de sus clientes, colaboradores externos, trabajadores, proveedores u otros terceros o que dicho comportamiento pueda ser constitutivo de infracción laboral, mercantil, civil, administrativa o penal) TWIM tratará los datos del usuario con la finalidad de efectuar un control y seguimiento pormenorizado de aquel, mediante la revisión de los ficheros electrónicos, mensajes de correo electrónico almacenados en su equipo (y recursos que lo componen) o remitidos desde el mismo y la identificación de las llamadas realizadas desde los terminales y dispositivos de telefonía y/o de envío de datos.

En particular y de acuerdo con las finalidades antedichas se informa al usuario de que sus datos de carácter personal podrán ser cedidos cuando ello sea necesario, así como cuando resulte legalmente obligatorio, a las Administraciones Públicas competentes en materia de control, inspección y potestad sancionadora, tal como Órganos de la Administración Laboral y Agencia Española de Protección de Datos, como a los Juzgados y Tribunales y el Ministerio Fiscal. Igualmente, TWIM deberá denunciar y poner en conocimiento de las Fuerzas y Cuerpos de Seguridad, así como de los Juzgados competentes, toda aquella información y datos que puedan revelar la presunta existencia de la comisión de una falta y/o delito al amparo de lo establecido en la Ley Orgánica 5/2010, del Código Penal.

Los tratamientos expuestos tienen carácter obligatorio y resultan imprescindibles a los fines indicados y en cumplimiento de la normativa vigente aplicable. En todo caso, TWIM garantiza que se llevarán a cabo con pleno respeto a la intimidad y privacidad del usuario y de acuerdo con los principios de necesidad, legitimidad, transparencia, proporcionalidad, menor injerencia, exactitud, seguridad y confidencialidad, tratando exclusivamente los datos que resulten necesarios para las finalidades expuestas en la presente comunicación.

Finalmente, se pone en conocimiento del usuario que sus datos podrán ser puestos a disposición de terceras entidades, cuándo dicho acceso sea necesario para la prestación de un servicio a TWIM en relación con las finalidades de tratamiento indicadas u otras finalidades inherentes a los procesos de trabajo y actividades de TWIM. En tales casos TWIM adoptará las medidas establecidas en la normativa vigente para garantizar que los terceros prestadores de servicios únicamente tratarán los datos conforme a las instrucciones de TWIM y que no los aplicarán o utilizarán con fin distinto, ni los comunicarán a otras personas.

Cualquier usuario puede ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose por escrito a TWIM en la siguiente dirección [datos.personales@twim.es]

15. FINALIZACIÓN DE LA RELACIÓN CON EL USUARIO

A partir de la finalización de la relación con TWIM, se revocarán los derechos de acceso del usuario cesante. En tal caso dicha autorización deberá ser emitida por TWIM.

Cuando un usuario finalice su relación con TWIM, deberá cesar en el uso, devolverlos y dejar intactas todas las herramientas, medios, sistemas, informaciones e instrumentos de trabajo, así como los archivos y documentos a los que haya tenido acceso por razón de sus funciones.

16. ACTUALIZACIÓN DE ESTE DOCUMENTO

Una copia actualizada de esta normativa se encuentra disponible en la carpeta de Documentos Compartidos de TWIM a la que cualquier usuario puede acceder mediante el uso de su ordenador. En caso de que se produzca un cambio relevante, el Responsable del Sistema lo notificará a los usuarios mediante el envío de un correo electrónico.

17. INCUMPLIMIENTO DE LAS OBLIGACIONES POR LOS USUARIOS

Cualquier incumplimiento de las normas y políticas establecidas por TWIM puede determinar la toma de sanciones y acciones legales oportunas por parte de TWIM conforme a lo establecido en el Reglamento y leyes vigentes aplicables.

En otros casos, TWIM atenderá a lo establecido en el correspondiente contrato con el usuario, así como, a los códigos civil, de comercio y laboral para determinar el alcance del incumplimiento y las consecuencias que se derivan del mismo para el usuario.