

Introducción

El Reglamento General de Protección de Datos de la Unión Europea (RGPD), en su artículo 24 establece como una obligación de responsabilidad proactiva del responsable del tratamiento, la necesidad de establecer las oportunas políticas de protección de datos, a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento.

Uno de los principios básicos de la protección de datos, recogido en el artículo 5.1.f) del RGPD, es el principio de seguridad.

Dicho artículo establece que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

En la misma línea, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), indica que, los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del RGPD, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable.

Fundación de la Comunidad Valenciana Centro de Investigación Príncipe Felipe (en adelante **CIPF**) ha implantado diversas medidas de seguridad de diversa naturaleza para garantizar el cumplimiento de la normativa de protección de datos.

Y, en este marco, CIPF ha elaborado la presente política de seguridad para los usuarios de datos personales del CIPF con el fin de establecer la seguridad organizativa para el acceso y uso de sistemas de información y tratamiento de datos personales.

A tal objeto, CIPF ha elaborado la presente política de obligado cumplimiento para todo su personal, así como cualquier otro personal usuario de los sistemas de información y tratamiento de datos personales de CIPF.

Aprobación de la política

La presente política ha sido aprobada por la Dirección General del CIPF.

Modificación de la política

La presente política puede ser modificada por la Dirección General del CIPF.

Objeto de la política

Constituye el objeto del presente documento establecer la política destinada a garantizar la seguridad y confidencialidad de los datos de carácter personal y en general, información, sistemas y redes de comunicaciones de CIPF.

Esta política ha sido elaborada e implantada en el marco del proceso de adaptación al RGPD de CIPF, en cumplimiento del principio de «responsabilidad proactiva» recogido en el RGPD.

REGLAS Y NORMAS:

a) Normas de uso de identificadores de usuario y contraseñas

- Los identificadores de usuario y contraseñas son personales e intransferibles puesto que otorgan derechos de acceso a medios, recursos y datos en ellos depositados en virtud de un acuerdo personal, adecuado al perfil profesional y a la función que desempeña la persona usuaria para CIPF.
- Queda prohibida la existencia de identificadores de usuario genéricos (o individuales de uso compartido) así como el uso de contraseñas compartidas o multiusuario.
- Queda prohibido comunicar los identificadores de usuario y las contraseñas de acceso a terceras personas.
- Cada persona usuaria será responsable única del mantenimiento de la confidencialidad de sus identificadores de usuario y de sus contraseñas.
- El formato y la longitud de las contraseñas deberán cumplir con los siguientes requisitos:
 - o Longitud mínima de ocho caracteres.
 - o Debe contener al menos un número, combinación de mayúsculas y minúsculas y un carácter especial.
- Toda contraseña deberá ser cambiada con una periodicidad de 6 meses.
- Cualquier incidencia que comprometa la confidencialidad deberá ser inmediatamente notificada a CIPF en el menor plazo de tiempo posible.

b) Normas de uso de los equipos informáticos (hardware)

- Está prohibido alterar los equipos informáticos o conectar otros (asistentes personales, impresoras, reconocedores de voz, módems, etc.) sin contar con la autorización por escrito de CIPF.

- Las normas establecidas en el presente documento son de aplicación tanto a los equipos informáticos fijos (equipos de sobremesa) como a los equipos informáticos portátiles (ordenadores portátiles, PDAs, teléfonos móviles, etc.) a los que la persona usuaria pudiera eventualmente tener acceso, así como a cualquier otro instrumento de transmisión telemática que CIPF pueda poner a disposición de la persona usuaria.
- Con respecto a los equipos informáticos portátiles es preciso recordar que la persona usuaria que tenga a su disposición alguno de ellos, debe extremar su precaución cuando haga uso de los mismos o los transporte fuera de las instalaciones de CIPF. Deben adoptarse todas las precauciones para evitar la pérdida o sustracción de estos equipos y en caso de que esta se produjese deberá darse inmediatamente aviso a CIPF.
- Los servicios WiFi, bluetooth o infrarrojos de los equipos portátiles sólo se habilitarán durante el tiempo en que la persona usuaria los necesite para desarrollar su actividad y aplicando la mayor seguridad disponible.
- Siempre que por cualquier motivo la persona usuaria abandone su puesto de trabajo bloqueará su equipo informático para evitar que terceros puedan acceder a los recursos y aplicaciones a las que la persona usuaria está autorizada.

c) Instalación de programas y almacenamiento de contenidos

- Es política de CIPF evitar cualquier tipo de actuación a través de los equipos informáticos y de comunicaciones puestos a disposición de la persona usuaria que pueda considerarse como atentatorio a la dignidad personal de otras personas. Por consiguiente, queda prohibido instalar o visualizar salvapantallas, fotos, videos, animaciones, y/o cualquier otro medio de reproducción o visualización de contenido ofensivo o atentatorio contra la dignidad de las personas.
- Los programas informáticos instalados en los equipos informáticos, así como los contenidos almacenados en los mismos son propiedad de CIPF o de otros terceros legítimos titulares que le han cedido la propiedad a CIPF o le han concedido una licencia de uso a CIPF.
- CIPF es el responsable de la instalación y configuración del equipo informático y del software asociado al puesto de trabajo de cada persona usuaria.
- Sólo se podrán instalar programas homologados y autorizados por CIPF.

- Queda prohibida la descarga e instalación de programas (gratuitos, versiones actualizadas de productos utilizados por CIPF, software freeware u otros productos, legales o no) sin la previa autorización de CIPF.
- Todos los equipos informáticos de CIPF tienen instalado el programa antivirus corporativo. No obstante, la persona usuaria deberá tener la máxima diligencia a la hora de ejecutar archivos procedentes de fuentes no conocidas. En caso de duda, la persona usuaria deberá abstenerse de ejecutar el archivo o programa y contactar directamente con CIPF.
- Bajo ninguna circunstancia se permite a la persona usuaria instalar, modificar o desactivar el programa antivirus instalado en los equipos. En caso en que se produzca una incidencia con el programa antivirus (compatibilidad con otras aplicaciones, virus y programas maliciosos) la persona usuaria deberá ponerlo en conocimiento de CIPF.
- Con carácter general está prohibida la utilización de programas de intercambio de ficheros, contenidos y/o la grabación de elementos sujetos a restricciones de propiedad intelectual (música, películas, programas de ordenador, etc.) en los equipos de CIPF y la utilización de soportes de almacenamiento de información propiedad de CIPF para tales fines.

d) Normas de uso de dispositivos móviles

- Esta normativa establece la manera correcta de utilizar recursos móviles facilitados por CIPF, entendiendo por éstos, sin carácter limitativo:
 - Teléfono móvil.
 - PIM (blackberry, Treo, Ipad y en general cualquier PDA con comunicación GSM, GPRS o UMTS en cualquiera de sus variantes).
 - Sistemas de comunicación móvil (modems PCMCIA o USB para la conexión a Internet de equipos portátiles).
 - Discos duros externos, dispositivos de almacenamiento USB.
- La conexión de cualquier tipo de dispositivo móvil de almacenamiento propiedad de la persona usuaria (PDAs, discos duros externos, llaves USB, lectores de mp3, relojes USB, cámaras de fotos digitales, teléfonos móviles, etc.) a los ordenadores personales y servidores de CIPF, queda sujeta autorización previa de CIPF en las condiciones que esta autorice.
- La solicitud de utilización de un dispositivo móvil de almacenamiento externo con fines laborales, profesionales o corporativos deberá ser dirigida a CIPF con indicación de la finalidad del uso que se le pretenda dar.

- En caso de ser autorizada su utilización, se tratará siempre de dispositivos autorizados por CIPF, no pudiendo ser utilizados para una finalidad distinta a la autorizada. La persona usuaria queda obligada en todo caso al uso razonable y equilibrado.
- La asignación de recursos móviles a la persona usuaria estará justificada por las condiciones de su puesto de trabajo y tareas que desarrolla.
- Los recursos móviles puestos a disposición de las personas usuarias de CIPF como una herramienta de trabajo más, cuya utilidad están sujetos a:
 - La facultad de CIPF de gestionar sus líneas móviles en razón de las necesidades del trabajo.
 - La facultad de CIPF de asignar con independencia entre otras personas usuarias los recursos móviles.
 - La titularidad de CIPF sobre los números asignados a los recursos móviles.
 - La política de predeterminación de llamadas salientes para comunicaciones con terceros (clientes y/o proveedores) preseleccionados.
 - La política de uso para acceso a Internet y/o correo electrónico del terminal.
 - Disponer de una facturación mensual con detalle por centro de los consumos de la persona usuaria del teléfono para facilitar el control presupuestario.
 - A establecer una política de regulación del tráfico de llamadas de cada línea según:
 - El horario de trabajo de la persona usuaria.
 - La cantidad de minutos a consumir.
 - Dicho control además podrá ser total y se podría impedir la salida de tráfico adicional después de su límite o dar avisos sobre las líneas que están llegando al límite.
- La persona usuaria que disponga de un recurso móvil de CIPF será depositaria y responsable del uso y custodia del mismo desde el momento en que se le entrega el terminal. CIPF no será responsable de cualquier tipo de sanción que a la persona usuaria se le pueda imponer por el uso indebido del terminal (v.gr por mantener conversaciones en lugares no permitidos y en especial cuando se encuentre conduciendo un vehículo).
- Además, y en particular, la persona usuaria que disponga de un recurso móvil proporcionado por CIPF en el marco de la relación profesional o laboral, deberán garantizar en todo momento:
 - El uso del mismo solo con fines laborales o profesionales como norma general.

- El uso ocasional con fines privados de un modo razonable, racional y moderado en el marco de lo establecido en la normativa vigente, en el presente documento siempre sin incurrir en los usos prohibidos. En todo caso el uso con fines privados no debe interferir con la productividad en la resolución de las tareas diarias y responsabilidades asignadas a la persona usuaria.
 - La persona usuaria borrará del terminal los correos electrónicos o sms o mms personales enviados o recibidos partir de 30 días después de su fecha de recepción.
 - Su custodia de forma segura.
 - La comunicación inmediata a CIPF del extravío y/o robo del terminal, así como un detalle de las circunstancias de dicho evento para que se proceda en su caso a realizar frente a los operadores y/o autoridades correspondientes las denuncias oportunas. Fuera del horario de trabajo la persona usuaria deberá comunicar directamente al operador de telecomunicaciones en su teléfono de atención al cliente para que se restrinja la línea inmediatamente y a CIPF en cuanto sea posible.
- Cualquier terminal y uso del servicio asignado por CIPF a la persona usuaria tiene carácter personal e intransferible. La persona usuaria queda obligada a mantener reservadas todas las claves de acceso al servicio que le sean facilitadas y no puede utilizar el servicio con la finalidad de enviar mensajes a terceros que puedan vulnerar la legalidad vigente.
 - La persona usuaria será única y totalmente responsable del contenido íntegro de los mensajes que envíe a través de su teléfono móvil, así como de los datos que facilite a terceros.

En el caso de servicios de mensajería móvil (sms/mms), queda prohibido:

- La creación, distribución o intercambio de contenidos ofensivos u obscenos, incluyendo material pornográfico.
- Mandar contenidos que promuevan la discriminación basada en raza, sexo, nacionalidad, edad, estado civil, orientación sexual o minusvalías.
- Mandar contenidos amenazantes o violentos.
- Intercambiar información corporativa propiedad de CIPF, secretos comerciales u otra información confidencial sin autorización de CIPF.
- Crear, enviar, reenviar o intercambiar mensajes comerciales no solicitados (SPAM), mensajes en cadena, solicitudes, anuncios o falsas alarmas.
- Crear, almacenar o intercambiar contenidos que violen las leyes de derechos de autor y derechos de uso y copia.

e) Normas de uso del correo electrónico

- Como regla general, CIPF suministra a cada una de las personas usuarias una dirección individual de correo electrónico corporativa. Es política de CIPF hacer un buen uso del correo electrónico, de conformidad con las leyes vigentes y las reglas del presente documento, teniendo en cuenta que las personas usuarias que utilicen el servicio están actuando en su propio nombre y representación, así como en el de CIPF.
- Queda prohibido modificar la configuración fija del cliente de correo electrónico implementada por CIPF.
- La persona usuaria debe poner el máximo cuidado al direccionar un mensaje para que llegue al destinatario correcto. La persona usuaria siempre comprobará que los destinatarios de los mensajes son los procedentes y adecuados para recibir la información contenida en el correo. La gramática y la ortografía de los mensajes debe ser chequeada antes de ser enviado.
- Los envíos de información a través del correo electrónico deberán estar firmados por la persona usuaria remitente de forma que cada persona usuaria deberá identificarse sin inducir a error al destinatario sobre su identidad.
- En caso de recibir un mensaje de correo electrónico destinado a otra persona, la persona usuaria lo notificará al remitente y acto seguido lo borrará. Ello se aplicará únicamente a aquellos remitentes considerados como fiables.
- La persona usuaria no podrá efectuar el envío de mensajes a varios destinatarios en lista abierta salvo que por razones de organización y gestión del trabajo sea preciso. En otro caso, los envíos deberán efectuarse a varios destinatarios siempre en copia oculta (cco/bcc) de forma que el destinatario de cabecera no pueda obtener información del resto de destinatarios. Ver para más dudas política de copia oculta publicada en Intranet.
- Todo correo electrónico enviado desde una cuenta de correo corporativa debe incluir una advertencia al pie configurada por CIPF. Si una persona usuaria detecta que dicha advertencia no se incorpora en sus envíos deberá comunicarlo a CIPF. Consultar con Departamento de Informática el texto al pie de los correos electrónicos.
- En ningún caso la persona usuaria debe eliminar dicha leyenda.
- Los envíos de correos electrónicos se realizarán de manera que no causen congestiones en la red corporativa.

- Queda terminantemente prohibido la creación, distribución o intercambio de contenidos ofensivos u obscenos, incluyendo material pornográfico, enviar contenidos que promuevan la discriminación basada en raza, sexo, nacionalidad, edad, estado civil, orientación sexual o minusvalías o enviar contenidos amenazantes o violentos. La recepción por la persona usuaria de un correo electrónico con dicho contenido deberá ser puesta en conocimiento de CIPF a fin de que ésta adopte las medidas legales oportunas.
- Asimismo, si la persona usuaria recibiera en su correo electrónico mensajes con contenido inadecuado deberá poner esta circunstancia en conocimiento de CIPF para la adopción de las medidas pertinentes.
- Queda prohibido a la persona usuaria intercambiar información propiedad de CIPF, secretos comerciales u otra información confidencial fuera de los casos expresamente autorizados por razón del cargo y desarrollo del trabajo.
- Por motivos de seguridad, el correo electrónico no podrá ser utilizado para enviar ni para contestar mensajes o cadenas de mensajes susceptibles de provocar congestiones en los sistemas de CIPF o que puedan introducir virus o implicar cualquier riesgo o problema en los sistemas, herramientas informáticas y tecnológicas de CIPF.
- El correo electrónico no podrá ser utilizado con fines comerciales ni lucrativos en beneficio de la persona usuaria.
- La persona usuaria cuidará en todo momento el lenguaje utilizado en sus comunicaciones, debiendo tener presente que en cada una de ellas compromete la imagen y el nombre de CIPF.
- La persona usuaria deberá prestar especial atención cuando utilice el correo electrónico, ya que todos los comentarios, opiniones o puntos de vista expresados a través del mismo pueden ser utilizados como prueba contra el remitente o contra CIPF, de la misma forma que las expresiones verbales o escritas, y en consecuencia, de las mismas pueden derivarse distintas responsabilidades.
- CIPF se reserva la potestad de eliminar periódicamente y previo aviso los correos electrónicos a partir de 6 meses después de la fecha de recepción/envío por motivos de espacio de almacenamiento en el servidor de correo.
- Se prohíbe la interceptación y/o uso no autorizado de mensajes o direcciones de correo electrónico de otras personas usuarias del sistema de información de CIPF, la modificación de un mensaje de otra persona usuaria sin su autorización y la usurpación de la identidad de otras personas usuarias en el envío de los mensajes.

- Queda prohibido igualmente el acceso al buzón de correo de otra persona usuaria sin autorización expresa de su titular.
- Si la persona usuaria va a estar ausente de su puesto de trabajo deberá notificarlo a CIPF si dicha circunstancia fuera conocida con anterioridad o posteriormente por si fuera necesario redireccionar su correo electrónico por razones de organización. A tales efectos el correo electrónico de la persona usuaria ausente será redireccionado a una cuenta determinada por CIPF, con objeto de que pueda ser leído para en su caso atender a las posibles gestiones.
- En estos casos, además, tanto la persona usuaria como en su caso el administrador del servidor de correo, podrán activar como acuse de recibo para los remitentes de los mensajes una comunicación en la que se indique que el destinatario del correo se encuentra ausente y en su lugar el mensaje de correo electrónico será leído y gestionado por otro empleado de la entidad.
- Queda prohibido tanto instalar cuentas de correo electrónico personales no corporativas como acceder a ellas a través del navegador de internet (webmail) salvo autorización previa y por escrito de CIPF.
- Los ficheros adjuntos a los correos de gran tamaño degradan las prestaciones del sistema de información. En este sentido, los archivos adjuntos mayores de 25 MB no serán aceptados por el servidor de correo, tanto para los enviados como para los recibidos. Si la persona usuaria necesita enviar un archivo adjunto mayor del señalado deberá solicitarlo a CIPF.
- Dado que tanto Internet como el correo electrónico son unas de las mayores fuentes de propagación e infección de virus informáticos ante cualquier sospecha de entrada de un virus informático, la persona usuaria cumplirá con la siguiente normativa:
 - No ejecutar jamás un ejecutable adjunto a un correo electrónico.
 - No abrir jamás los mensajes de correo provenientes de fuentes desconocidas.
 - No abrir jamás ningún adjunto sin asegurarse de que no está infectado, venga de quien venga.
 - En caso de abrir documentos de Microsoft Office (Word, Excel...), hacerlo siempre sin ejecutar las macros salvo que se tenga la certeza de que no son dañinas. Es posible que contengan virus.
 - En todo caso y a la menor sospecha o certeza de cualquier amenaza comunicarlo de inmediato a CIPF.
- Queda prohibida la suscripción a listas de correo, revistas, diarios, blogs, chats, publicaciones, grupos de noticias u otros servicios similares. Solo serán admisibles si están directamente relacionadas con las actividades de CIPF.

- La persona usuaria únicamente podrá utilizar la cuenta de correo electrónico de CIPF para fines particulares o personales, siempre que ese uso garantice el cumplimiento de la normativa vigente, siga las normas reflejadas en este documento y las siguientes reglas:
 - La persona usuaria podrá utilizar el correo electrónico con fines privados siempre que haga un uso ocasional, razonable, racional y moderado del mismo, en el marco de lo establecido en el presente documento y sin incurrir en los usos prohibidos.
 - El uso del correo electrónico no debe interferir con la productividad en la resolución de las tareas diarias y responsabilidades asignadas.
 - La persona usuaria en todo caso se encargará de borrar periódicamente aquellos correos particulares y privados que no tengan relación con su desarrollo profesional y/o laboral.
- Asimismo, se prohíbe a la persona usuaria la distribución o envío -sin carácter limitativo- de ficheros, archivos, informaciones y datos o su recepción a través de una dirección de correo electrónica privada de la persona usuaria o de un tercero ajena a CIPF o su colocación en Internet o cualquier otra red pública de comunicación.

f) Normas de uso de Internet

- La persona usuaria debe seguir siempre una conducta educada honesta y correcta en Internet, respetar los derechos de copia, los acuerdos de licencia de software, derechos de propiedad, privacidad y prerrogativas de terceros.
- La persona usuaria deberá acceder a Internet desde los medios puestos a su disposición por CIPF y utilizando sus claves, contraseñas y códigos de acceso.
- Queda prohibido modificar la configuración fija del navegador de Internet implementada por CIPF.
- La persona usuaria no deberá burlar los sistemas que protegen la seguridad de otros recursos de red o la privacidad de otras personas usuarias en su navegación por Internet.
- En el caso de que el acceso a ciertas páginas web con ciertos contenidos se encontrara restringido por medios técnicos, la persona usuaria no está autorizado a eliminar, modificar o saltarse ninguna de dichas restricciones implementadas por CIPF.
- La persona usuaria no podrá descargar copias de páginas web para su visualización "off-line".

- La persona usuaria no podrá acceder o utilizar los servicios y contenidos de Internet de forma contraria a las condiciones generales de uso y/o las condiciones particulares que regulen el uso de cada página web, un determinado servicio y/o contenido, y en perjuicio o con menoscabo de los derechos del resto de persona usuarias.
- La persona usuaria no podrá utilizar Internet de manera que viole la legislación vigente. Tampoco podrá acceder a páginas con contenido sexual, erótico, pornográfico, discriminatorio en función de raza, sexo, religión, nacionalidad, tendencias sexuales, difamatorios, lesivos, violentos, amenazantes u ofensivos para personas, entidades, instituciones o empresas o que supongan una infracción civil, penal, administrativa o fiscal, o que atenten contra la propiedad industrial o intelectual de CIPF o de terceros. Tampoco está permitido el acceso a páginas de software ilegal, “hackers” y “crackers”, y en general a toda página sospechosa de estar al margen de la legislación vigente en la materia.
- La persona usuaria no podrá utilizar 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.
- La persona usuaria debe minimizar el tráfico de la red innecesario que pueda interferir en la capacidad del resto de equipos y persona usuarias de utilizar de forma eficaz los recursos de red de CIPF.
- La persona usuaria queda informada de la existencia de filtros o sistemas de bloqueo que avisan a la persona usuaria acerca de la imposibilidad de acceder a determinados “sitios” de Internet por motivos como ser considerados contrarios a la legislación vigente, la moral, las buenas costumbres y el orden público.
- Queda prohibido el uso de programas de redes *peer to peer* (P2P) tipo emule, edonkey, kaza, win-mx, overnet, soul seek, o cualquier otra variación destinada al intercambio de archivos.
- Queda prohibido escuchar música por Internet, bajar o visualizar/escuchar video clips o archivos de música o participar en chats de sitios web que no respeten la normativa de propiedad intelectual e industrial.
- La persona usuaria únicamente podrá utilizar los servicios de Internet de CIPF para fines particulares o personales, siempre que ese uso garantice el cumplimiento de la normativa vigente, siga las normas reflejadas en este documento y las siguientes reglas:
 - Que el uso sea ocasional, razonable, racional y moderado en el marco de lo establecido en el presente documento y sin incurrir en los usos prohibidos.

- Que el uso no interfiera con la productividad en la resolución de las tareas diarias y responsabilidades asignadas.
- Que no dañe la reputación de CIPF.
- Que no reduzca la productividad del empleado o sus compañeros.
- Que no afecte al rendimiento del sistema de información de CIPF.

g) Normas de uso de datos de carácter personal

La persona usuaria queda informada de que, en cumplimiento de lo establecido en la normativa vigente sobre protección de datos personales (Reglamento General de Protección de Datos, en adelante RGPD y Ley Orgánica de protección de datos y garantía de los derechos digitales, en adelante LOPDGDD) debe cumplir las siguientes normas establecidas por CIPF en relación con los datos de carácter personal contenidos en los soportes, documentos, ficheros temporales o no, tratamientos, programas y en su caso, equipos y dispositivos empleados para su tratamiento, cualquiera que sea el modo en que se organiza o utiliza la información (automatizados, no automatizados o parcialmente automatizados).

Todos los datos personales están protegidos por el RGPD y sometidos al principio de confidencialidad de forma que la persona usuaria queda obligada al deber de secreto y confidencialidad de cualquier dato de carácter personal al que haya tenido acceso, tanto durante la vigencia de su relación con CIPF como tras la finalización de la misma.

Cualquiera que sea el sistema de tratamiento utilizado en relación con los datos de carácter personal sujetos a protección -automatizado o no automatizado- la persona usuaria deberá tener en cuenta las normas a continuación establecidas a continuación.

- Queda prohibido facilitar el acceso a datos, a soportes que los contengan o a recursos del sistema de información que los trate a terceros ajenos a CIPF sin tener autorización previa de CIPF.
- Queda prohibida la contratación de terceros que necesiten acceder y tratar datos personales contenidos en los sistemas y equipos de CIPF sin tener autorización previa y por escrito de CIPF.
- Aquellos ficheros temporales o copias de documentos que la persona usuaria hubiese creado exclusivamente para la realización de trabajos temporales o auxiliares deben garantizar las medidas de seguridad establecidas por CIPF y ser borrado o destruido de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- La persona usuaria debe tener acceso únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones. Queda prohibido acceder e intentar acceder a datos y recursos no autorizados de tratamiento de datos personales.
- La persona usuaria respetará que exclusivamente el personal autorizado para ello por CIPF podrá conceder, alterar o anular accesos sobre los datos y recursos de tratamiento, conforme a los criterios establecidos por CIPF.
- En caso de que la persona usuaria necesite acceder a nuevos datos y recursos a los que actualmente no tiene acceso realizará una solicitud a CIPF mediante documento escrito en el que se solicite de forma motivada la necesidad de acceso a ellos.
- El acceso lógico a los datos se llevará a cabo mediante el uso de nombres de usuario y contraseñas. Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema deben ser estrictamente confidenciales y personales y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada a CIPF para su subsanación en el menor plazo de tiempo posible.
- La persona usuaria queda obligada a cambiar la contraseña de acceso al sistema con la periodicidad establecida en la presente política.
- Cada puesto o estación de trabajo es responsabilidad de la persona usuaria a la que se ha asignado y a la que se ha autorizado a ocuparlo 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 otras personas usuarias no autorizadas para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Siempre que la persona usuaria vaya a desechar algún documento o soporte que contenga datos de carácter personal deberá proceder a su destrucción o borrado mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
- La persona usuaria deberá prestar especial atención al llamado “papel sucio”. Nunca se arrojará papel con información impresa a la papelera sin haber sido sometido a un proceso de destrucción –tritadora de papel, rotura a mano en el máximo número de trozos posibles- de manera que la información quede totalmente ilegible. Existen destructoras de papel en el departamento de Administración.

- Para la ejecución de las siguientes actuaciones, la persona usuaria deberá dirigirse a CIPF para solicitar la correspondiente autorización dado que, exclusivamente el personal autorizado por CIPF podrá llevar a cabo las siguientes acciones:
 - Cuando la persona usuaria necesite almacenar o tratar datos personales en dispositivos portátiles o fuera de los locales de CIPF.
 - Cuando la persona usuaria necesite llevar a cabo un almacenamiento o tratamiento de datos personales fuera de los locales de CIPF.
 - Cuando la persona usuaria necesite llevar a cabo alguna salida de soportes o documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico.
 - En caso de que la persona usuaria necesite ejecutar procedimientos de recuperación de datos.

- La persona usuaria deberá comunicar al responsable de CIPF cualquier incidencia que afecte, haya afectado o pueda afectar a la seguridad de los datos. La notificación de cualquier incidencia será notificada por la persona usuaria en el momento en que se ha producido mediante correo electrónico, indicando al menos la siguiente información:
 - El tipo de incidencia, incluyendo: naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
 - El momento en que se ha producido, o en su caso, detectado.
 - Las posibles consecuencias de la violación de la seguridad de los datos personales, incluyendo el alcance de los daños y los efectos que se hubieran derivado de la misma.
 - Las medidas correctoras aplicadas –en su caso- o propuestas para poner remedio a la violación de los datos, incluyendo si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
 - Y cualquier otra información relevante.

- En el traslado de la documentación la persona usuaria adoptará las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

- La persona usuaria deberá llevar a cabo el archivo de los soportes o documentos que contengan datos personales en sistemas no automatizados de acuerdo con los criterios previstos en su respectiva legislación, que en todo caso deberán garantizar:
 - o La correcta conservación de los documentos
 - o La localización y consulta de la información
 - o Y posibilitar el ejercicio de los derechos
 - o La identificar el tipo de información que contienen; utilizando sistemas de etiquetado comprensibles que permitan a las personas con acceso autorizado a los citados soportes y documentos identificar su contenido y, que dificulten la identificación para el resto de personas.
 - o Los soportes deben ser inventariados y ser accesibles únicamente por el personal autorizado.

- En aquellos casos en los que no exista norma aplicable, la persona usuaria deberá seguir para el archivo los criterios y procedimientos de actuación establecidos por CIPF.

- Cuando las características físicas del soporte imposibiliten el cumplimiento de lo anterior, la persona usuaria deberá comunicar esta circunstancia a CIPF.

- La persona usuaria solo podrá almacenar documentos que contengan datos de carácter personal en dispositivos de almacenamiento que dispongan de mecanismos que obstaculicen su apertura. No obstante, cuando las características físicas de aquéllos no permitan adoptar esta medida, la persona usuaria lo pondrá en conocimiento de CIPF para que se adopten medidas que impidan el acceso de personas no autorizadas.

- Mientras la documentación que contiene datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona usuaria que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida personas no autorizadas.

- La persona usuaria deberá solicitar a CIPF soluciones de cifrado de datos personales en el ejercicio de su trabajo que almacene en sus dispositivos portátiles, cuando dichos datos personales se refieran a las siguientes categorías: aquellos 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 orientaciones sexuales de una persona física, datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas (en adelante, categorías especiales de datos).

- Queda prohibido el almacenamiento y tratamiento de datos de carácter personal de los mencionados en el punto anterior en dispositivos portátiles de la persona usuaria que no permitan su cifrado. En caso de que sea estrictamente necesario la persona usuaria deberá ponerlo en conocimiento de CIPF a fin de que en su caso sea debidamente autorizado dicho tratamiento previa adopción de determinadas garantías.
- Queda prohibida toda transmisión de categorías especiales de datos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas sin que dichos datos sean sometidos a algún proceso de cifrado o bien se utilice cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
- La persona usuaria únicamente podrá almacenar documentos que contengan categorías especiales de datos personales en armarios, archivadores u otros elementos que se encuentren en áreas en las que el acceso esté protegido con puertas de acceso y dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. En otro caso, la persona usuaria pondrá en conocimiento del responsable de CIPF la necesidad de almacenar documentos con categorías especiales de datos en ubicaciones seguras a fin de que se adopten las debidas medidas por CIPF.

En todo caso CIPF pone en conocimiento de la persona usuaria que está terminantemente prohibido en relación con el tratamiento de datos personales:

- Acceder o facilitar los accesos de terceras personas a los sistemas de información automatizados y no automatizados, tanto a nivel físico como lógico, sin estar previamente autorizadas por CIPF.
- Facilitar cualquier soporte o documento con datos de carácter personal a personas no autorizadas por CIPF.
- Trasladar soportes o documentos con datos personales fuera de los locales donde está ubicado sin autorización de CIPF.
- Realizar trabajos fuera de los locales de la ubicación de los ficheros definida por CIPF sin autorización de CIPF, que solo se otorgará si hay garantías de seguridad correspondientes al tipo de información objeto de tratamiento.
- Enviar información contenida en los ficheros de datos a través de ningún tipo de sistema de transmisión de información sin autorización de CIPF.
- Romper el secreto profesional respecto de los datos personales conocidos, cualquiera que fuere el soporte de tratamiento aún después de terminada la relación con CIPF.

- Realizar cualquier tipo de copia de respaldo de los ficheros a los que la persona usuaria tiene acceso, en cualquier tipo de soporte (cintas, discos, CD-Rom, DD, dispositivos externos de almacenamiento u otro medio físico, etc.) sin estar autorizado por CIPF.
- Copiar o guardar cualquier copia de datos personales, total ni parcialmente, ni de cualquier otro material, información o documentación cualquiera que sea el soporte en el que se encuentren los datos, fuera de los procedimientos y con las medidas de seguridad establecidas por CIPF.

h) Confidencialidad de la información y deber de secreto

De conformidad con la legislación vigente en materia de protección de datos personales quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, pudiendo ser constitutivas de delitos y/o falta contra los bienes jurídicos protegidos, determinadas conductas de revelación de datos cometidas por las personas obligadas al deber de secreto.

Asimismo, tienen el carácter de confidencial a efectos de la política de seguridad de CIPF toda la información y datos (cualquiera que sea el lugar y forma de acceso a los mismos, tal como instalaciones, dependencias, recursos, sistemas, documentos en soporte papel, documentos electrónicos) incluyendo y sin que implique restricción y/o esta enumeración tenga carácter limitativo de carácter económico, financiero, industrial, técnico, comercial, estratégico, administrativo, datos de carácter personal, datos de cualquier otra naturaleza, metodologías, algoritmos, códigos de desarrollo informático, programas de ordenador, dibujos, grabaciones, documentos y material titularidad de CIPF y/o de terceros custodiada por dicha entidad, los documentos y trabajos desarrollados por la persona usuaria para el desarrollo de proyectos propios de CIPF y/o de clientes de CIPF, ya se trate todo lo anterior de informaciones y datos contenidos en pasadas, presentes y futuros, investigaciones, desarrollos, actividades de negocio (incluyendo toda la información de o sobre clientes de CIPF, personas físicas y/o jurídicas), productos, servicios, y conocimiento técnico de CIPF (bien sea revelado oralmente, en forma de documento -electrónico o no-, demostración o de cualquier otro modo), todo lo cual se denominará en el presente documento de forma genérica como "Información Confidencial".

Será igualmente considerada Información Confidencial, aquella que resulte de cualquier proceso o tratamiento tomando como base la descrita en el apartado anterior.

Respecto de la "información confidencial" la persona usuaria queda obligada al cumplimiento de las siguientes normas y obligaciones:

- Será potestad de CIPF (i) determinar en cada caso la necesidad de proporcionar a la persona usuaria la Información Confidencial de CIPF en forma, condiciones, soportes y finalidad o (ii) en otro caso, de no ser necesaria para la prestación de sus servicios profesionales o desarrollo de su trabajo, establecer las medidas oportunas para impedir el acceso a dicha información y/o en su caso limitar el acceso de la persona usuaria la información confidencial, a los soportes que la contengan o a los recursos del sistema de información donde se almacene, para la realización de trabajos que no impliquen el tratamiento de la Información Confidencial.
- Las obligaciones contempladas en este documento respecto al deber de secreto y confidencialidad que incumbe a la persona usuaria que intervenga en cualquier fase del tratamiento de Información Confidencial y al deber de guardarla, perdurarán de forma indefinida, aún finalizada su relación laboral o profesional con CIPF.
- Este deber de secreto incluye la prohibición de utilizar o comunicar Información Confidencial con un fin distinto al establecido por CIPF.
- La Información Confidencial de CIPF debe ser utilizada por la persona usuaria solo en el contexto de su relación jurídica y contrato laboral o profesional de prestación de servicios suscrito con CIPF y para el fin para el que fue revelada.
- La persona usuaria estará obligada a tratar la Información Confidencial que CIPF pone a su disposición, siguiendo las instrucciones de seguridad que CIPF determine, le comunique y ponga a su disposición sin perjuicio de la obligación de la persona usuaria -en calidad de depositario de la Información Confidencial- de velar por la seguridad de y adoptar por iniciativa propia las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de la Información confidencial y evite su alteración, pérdida, tratamiento o acceso no autorizado.
- Cualquier desvío de Información Confidencial producida por la vulneración del deber de secreto y confidencialidad y/o la falta en las medidas de seguridad mencionadas en el apartado anterior, será responsabilidad de la persona usuaria que la cause.
- Se considerará desvío de Información Confidencial, toda comunicación a terceras personas, ya sean físicas o jurídicas, que no fuesen los destinatarios legítimos de la mencionada información.
- La persona usuaria no debe permitir el acceso a Información Confidencial a terceros sin el consentimiento expreso y por escrito de CIPF.

- La persona usuaria no está autorizada a copiar de ninguna forma técnicamente posible y almacenar fuera de los procesos controlados y autorizados de CIPF, la Información Confidencial puesta a su disposición por CIPF sin el consentimiento expreso y escrito de CIPF.
- CIPF se reserva el derecho de restringir el acceso de la persona usuaria la Información Confidencial de CIPF o de terceros.
- La persona usuaria deberá devolver a CIPF y/o destruir a criterio de CIPF, incluyendo copias, toda la Información Confidencial cuando así se lo solicite CIPF, o al finalizar la relación jurídica laboral o profesional mantenida con CIPF.
- No será concedido a la persona usuaria ningún derecho en virtud de este documento fuera de los atribuidos explícitamente en él, respecto de la Información Confidencial que seguirá siendo propiedad de CIPF y/o de terceros:
 - El trabajo realizado para CIPF por la persona usuaria se considera Información Confidencial, especialmente cuando este tenga relación con el uso de datos de carácter personal.
 - Salvo acuerdo expreso en contrario con la persona usuaria, esta no tiene ningún derecho de propiedad ni especialmente derecho de propiedad intelectual ni industrial sobre la Información Confidencial de CIPF ni derecho de propiedad sobre los soportes en que CIPF ponga a su disposición la Información Confidencial.
- Cualquier solicitud de Información Confidencial que un tercero (persona física o jurídica) efectúe a la persona usuaria, deberá ser previamente comunicada a CIPF y no se accederá a la mencionada solicitud sin el preceptivo permiso de CIPF.
- En el caso de que la persona usuaria reciba una orden judicial, administrativa, o algún otro proceso judicial solicitando Información Confidencial sobre CIPF, éste debe informar inmediatamente a CIPF del alcance de dicha orden o proceso y a partir de ese momento cumplirá con el mismo hasta donde le exija la ley.
- La persona usuaria solo revelará la Información Confidencial de CIPF estrictamente requerida por la autoridad judicial y/administrativa, informando a CIPF en todo momento, con claridad y transparencia del estado del proceso y de la Información relativa a CIPF contenida en él.
- En el supuesto de que la persona usuaria destine la Información Confidencial a una finalidad diferente a la establecida por CIPF, la comunique o utilice incumpliendo las estipulaciones del presente documento, responderá personalmente de las infracciones en que hubiera incurrido además de su responsabilidad disciplinaria.

A efectos de lo establecido en este documento y sin perjuicio de las acciones legales que corresponda a CIPF, se entenderá como ruptura de la obligación de confidencialidad y competencia desleal el uso de la Información Confidencial por la persona usuaria en otras empresas una vez se deja de trabajar para CIPF.

i) Finalización de la relación entre CIPF y la persona usuaria

CIPF pone a disposición de la persona usuaria la infraestructura y los recursos adecuados para la realización de sus funciones. No obstante, a partir de la finalización de la relación jurídica que ampara el acceso de la persona usuaria los recursos e información de CIPF, la persona usuaria no podrá tener acceso a dicha infraestructura y recursos incluyendo cualesquiera archivos e informaciones incluidos en los mismos, salvo autorización por escrito en sentido contrario.

Cuando una persona usuaria finalice su relación con CIPF, deberá borrar cualquier información privada y doméstica y dejar intactos todos los archivos y documentos que hayan tenido un fin profesional o laboral.

En el supuesto de que existieran archivos de carácter privado o doméstico no eliminados por la persona usuaria, se procederá a la eliminación de los mismos bajo la supervisión del personal responsable de CIPF respetándose en todo caso las garantías legales.

En el momento en que se extinga la relación de la persona usuaria con CIPF, y salvo autorización expresa en sentido contrario, se interrumpirá el acceso al buzón de correo electrónico puesto a disposición de la persona usuaria. No obstante, con el objeto de salvaguardar la continuidad en las relaciones de CIPF con todas aquellas personas físicas o jurídicas con quienes CIPF mantiene relaciones profesionales o comerciales, el personal autorizado de CIPF podrá adoptar las medidas necesarias para reenviar los mensajes profesionales o comerciales a aquellas otras personas usuarias que se determine dentro de cada departamento.

En el supuesto en que finalizada la relación con CIPF la persona usuaria tenga en su poder determinados medios, recursos o instrumentos de trabajo tendrá que devolverlos inmediatamente a CIPF en buen estado de uso y conservación.

Información sobre el tratamiento de datos personales de la persona usuaria derivado de la aplicación de la normativa de seguridad

Responsable del tratamiento: Fundación de la Comunidad Valenciana Centro de Investigación Príncipe Felipe(en adelante CIPF) con domicilio en C/ D' Eduardo Primo Yúfera, número 3, 46012 Valencia, teléfono de contacto 963289680 y dirección electrónica de contacto info@cipf.es.

Dirección electrónica de contacto del delegado de protección de datos:
privacy@cipf.es.

Fines del tratamiento: Con base jurídica en el cumplimiento de las normas vigentes sobre protección de datos de carácter personal y seguridad de los sistemas así como en el marco de la relación laboral con la persona usuaria, y en el interés legítimo de CIPF de cumplir con las normas internas de seguridad para prevenir riesgos y daños y garantizar el funcionamiento de los procesos y actividad de la empresa, la finalidad del tratamiento de los datos es la verificación, revisión y evaluación regular de la seguridad y confidencialidad de los sistemas, redes, información y datos personales que CIPF ponen a disposición de la persona usuaria para el desarrollo de su trabajo, así como prevenir riesgos, actuar frente a incidentes y cumplir frente a terceros, incluidas las autoridades competentes, las obligaciones y responsabilidades legales.

Necesidad del tratamiento: El tratamiento de los datos personales, según lo indicado constituye un requisito legal necesario en cumplimiento del deber de CIPF de velar por la seguridad y confidencialidad de los sistemas, información y datos personales, de acuerdo con sus obligaciones legales y normas internas de empresa.

Plazo de conservación de datos: Los datos personales de la persona usuaria se conservarán por CIPF durante toda la vigencia de la relación laboral y/o profesional con la persona interesada y finalizada esta, durante los plazos indicados en las normas aplicables para el cumplimiento de obligaciones y atención de responsabilidades por CIPF.

Destinatarios de los datos: Los datos personales serán comunicados a las Autoridades Públicas y Órganos Judiciales competentes por razón de la materia, Ministerio Fiscal, así como auditores y terceros clientes de CIPF que soliciten la verificación de las “garantías suficientes” en el cumplimiento por CIPF de sus obligaciones legales y contractuales.

Encargados del tratamiento: Terceras empresas externas a CIPF (denominados encargados del tratamiento), tendrán acceso a los datos de la persona usuaria con el fin de prestar servicios a CIPF. Los datos serán puestos a disposición de dichos encargados del tratamiento al amparo de un contrato de prestación de servicios y otro de encargo de tratamiento con la obligación de seguir las instrucciones de tratamiento de CIPF, guardar la confidencialidad, devolver y/o destruir los datos a la finalización del servicio, quedando prohibido el tratamiento de los datos para fines propios de los encargados del tratamiento.

Transferencias internacionales de datos: Salvo obligación legal, los datos de la persona usuaria no serán transferidos internacionalmente.

Derechos: Las personas interesadas pueden ejercitar sus derechos de acceso, rectificación, cancelación o supresión y oposición, limitación del tratamiento, portabilidad y derecho a no ser objeto de una decisión basada en el tratamiento automatizado de sus datos personales enviando una petición escrita a CIPF aportando una copia de su DNI o documento válido en Derecho para acreditar su identidad, a cualquiera de las siguientes direcciones:

Dirección postal: calle D' Eduardo Primo Yúfera, número 3, 46012 Valencia

Dirección electrónica: info@cipf.es

Otros derechos: Además, el usuario queda informado del derecho que le asiste a presentar una reclamación ante una Autoridad de control (en España la Agencia Española de Protección de Datos (en adelante AEPD), en particular, cuando consideren que no han obtenido satisfacción en el ejercicio de sus derechos, a través de www.agpd.es o en la siguiente dirección C/ Jorge Juan, 6. 28001 – Madrid, y/o teléfono de contacto 912 663 517. En todo caso, y con carácter voluntario y previamente a solicitar la tutela de la AEPD, la persona usuaria podrá contactar con el delegado de protección de datos de CIPF para que su reclamación sea atendida a través de privacy@cipf.es.

Obligaciones del personal

Todo el personal señalado en el apartado anterior tiene la obligación de conocer y cumplir la presente política y normativas, medidas y procedimientos derivados de la misma.

El incumplimiento de la presente política o la normativa, medidas y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Consultas

Cualquier consulta o sugerencia en relación con la presente política, podrá ser consultada al/ a la Delegado/a de Protección de Datos.

Efectividad

La presente normativa entrará en vigor el día de su aprobación y quedará publicada para conocimiento y cumplimiento de todos los empleados en el sitio web del CIPF.

Esta política sustituye a cualquiera anterior ya aprobada y publicada por CIPF dejándola sin vigencia. Además, la presente política podrá ser modificada en el futuro de acuerdo con la evolución de CIPF, cambios tecnológicos y cambios legales que se produzcan, a cuyos efectos CIPF procederá a notificar a la persona usuaria el documento actualizado para su cumplimiento. La última versión publicada del mismo e insertada en la carpeta indicada, siempre será la vigente.