Confidencialidad, Funciones y obligaciones del personal de Cáritas

Nombre: _____ DNI. / NIE: _____

Mediante el presente documento, CÁRITAS DIOCESANA DE SEGORBE-CASTELLÓN cumple su deber de informar a todo el personal sobre la confidencialidad, el deber de secreto y sobre las normas de seguridad y protección de datos de carácter personal.

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

En ocasiones, los miembros mencionados desempeñan sus funciones en locales vinculados a Cáritas Interparroquiales o Cáritas Parroquiales. Esa circunstancia no impedirá la aplicación de este documento, aunque será la Cáritas Interparroquial o Parroquial correspondiente la encargada de disponer todo lo concerniente a equipos e infraestructura.

# Sumario

# I. CONFIDENCIALIDAD Y DEBER DE SECRETO

Todo el personal se compromete a:

1. No revelar a ninguna persona ajena a la entidad sin el consentimiento de la misma, la información 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 a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en la entidad 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, voluntario o colaborador y que no fuera necesaria para el desempeño de sus funciones en la entidad.

4. Cumplir, en el desarrollo de sus funciones en la entidad, 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, de voluntariado o de prestación de servicios que le une con la entidad.

El personal será responsable, ante la entidad 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 la entidad, 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 la entidad 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 por parte del personal, voluntario, alumno en prácticas y colaboradores de la entidad, el trabajador, voluntario, alumno en prácticas o colaborador declara que lo ha leído y comprendido en toda su extensión.

Firmado:

El trabajador / voluntario / alumno en prácticas /colaborador

En _____, a _____ de _____ de 20__

# II. MEDIDAS DE SEGURIDAD Y PROHIBICIONES

Las siguientes medidas de seguridad son de obligado cumplimiento para todo el personal de la entidad (personal laboral, voluntariado, estudiantes en prácticas y colaboradores) 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 todo el personal de la entidad (personal interno y externo, voluntarios, así como estudiantes en prácticas o colaboradores) que tenga acceso a los datos ~~automatizados~~ de carácter personal y a los sistemas de información.

## A. Soportes de información

### 1. Documentación en papel.

- Cuando la documentación con datos de carácter personal no se encuentre archivada, 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.

- Las copias o reproducciones desechadas deberán destruirse, 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. Contraseñas.

- Se evitarán nombres comunes o fáciles de adivinar.

- No se dará la contraseña a nadie ni se utilizará la contraseña de otra persona.

- No hacer uso de la opción de guardar la contraseña en ningún dispositivo ni programa informático.

## 3. Ordenadores de sobremesa y portátiles.

- En el caso de trabajar con datos personales se utilizarán las carpetas del servidor de la entidad siempre que estén disponibles. Se prohíbe almacenar en los ordenadores datos personales sin autorización.
- Los ordenadores de la entidad son para fines estrictamente laborales y por tanto no se utilizarán para fines particulares. La entidad podrá controlar 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 personal 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.
- No está permitido instalar *motu proprio* ningún producto informático o APP. Todas aquellas aplicaciones necesarias serán autorizadas por el administrador del sistema e instaladas por personal autorizado para ello. También está prohibido alterar la configuración del sistema, dispositivo y aplicativos de gestión.
- Quien necesite utilizar su dispositivo personal deberá comunicarlo previamente a su superior. En caso de autorizarse, el interesado deberá implementar las medidas de seguridad oportunas que garanticen la seguridad y confidencialidad de sus datos, así como firmar los documentos oportunos.

## 4. Soportes de almacenamiento (lápiz USB, discos duros externos, etc.)

- 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 (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. Móviles corporativos (incluyendo tablets y PDA’s).

- El dispositivo es para fines estrictamente laborales y por tanto no se utilizará para fines particulares. La entidad podrá monitorizar 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 la entidad en el dispositivo, así como el sistema de bloqueo, el sistema de borrado remoto, el cifrado de datos o cualquier otro.
- Queda totalmente prohibida cualquier modificación o reconfiguración 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 en los dispositivos móviles datos personales catalogados como categorías especiales de datos, como 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 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 entidad, 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 la entidad.
- Los equipos telefónicos fijos y móviles, así como el fax son propiedad de la entidad, 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.Categorías especiales en dispositivos

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 Caritas Diocesana de Segorbe-Castellon.

### 7. Salida de soportes informáticos.

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

## B. Hábitos seguros de trabajo

### 8. Navegación por Internet y correo electrónico

Respecto al uso de Internet y de la cuenta de correo electrónico facilitada por la entidad, esta será de uso y desarrollo exclusivamente de las funciones laborales o propias del voluntariado del personal. No podrá utilizarse la cuenta de correo electrónico proporcionada por la entidad para otros fines. La entidad podrá acceder al contenido de los correos electrónicos y comprobar el historial de navegación en Internet.

La entidad, 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 la entidad, se observarán las siguientes normas:

- Respecto a las contraseñas, se seguirá lo indicado en el apartado “Contraseñas” de este documento.
- 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 la entidad, 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, el personal 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 o voluntarios 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 la entidad:

- Al finalizar, cerrar la sesión de webmail y borrar el historial de navegación.
- No deberá guardar datos en terminales o soportes ajenos a la entidad, 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. Trabajo en la nube

- Queda prohibido el uso de aplicaciones en la nube para compartir documentos o para desarrollar un trabajo no presencial, a no ser que no estén previamente autorizadas por el administrador del sistema. Algunas de estas aplicaciones 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 la entidad de una serie de medidas y cautelas impuestas por la normativa.
- Para el manejo de datos personales, se recomienda el trabajo remoto en una carpeta del servidor (conexión VPN).
- Cuando la conexión VPN no esté disponible, se autoriza el uso de Google Drive únicamente a través de las cuentas facilitadas por Cáritas Diocesana de Segorbe-Castellón dentro de su dominio (terminadas en @caritas-sc.org).

## 10. Ficheros temporales.

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.

## 11. Nuevos tratamientos de datos.

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

## 12. 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.

# C. Entrada y salida de datos

## 12. Recogida de datos personales

- Los datos personales que se recojan deben contar con la firma del consentimiento por parte de la persona interesada (participante, persona voluntaria, personal laboral, socio o donante…).

- En los casos en que la firma del consentimiento no sea posible (p. ej. trípticos de socios o formularios web) se buscarán maneras alternativas para recabar el consentimiento (marcar casillas en formularios web, hacer llegar al interesado una copia del consentimiento…).
- Los datos personales se podrán recabar personalmente, por correo postal o electrónico o por la página web de la entidad. En ningún caso se podrán recabar datos personales vía Whatsapp u otras aplicaciones no autorizadas.
- Las grabaciones de imágenes y sonido constituyen un dato personal, por lo que se deberá recabar el consentimiento, en especial de los participantes, mediante el correspondiente documento.
- Cualquier soporte informático con datos personales 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.

## 13. Envío de datos personales a terceros

- Queda terminantemente prohibido facilitar a persona alguna ajena a la entidad ningún soporte conteniendo datos, a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.
- En el ejercicio de sus funciones, el personal podrá enviar información únicamente a los terceros a los que el interesado haya autorizado a tales efectos en su hoja de consentimiento.
- Dicho envío de datos personales será registrado obligatoriamente. A tal efecto, se efectuará vía correo electrónico y se enviará con copia oculta al correo registrodesalida@caritas-sc.org, que actuará como registro de todos los envíos efectuados por el personal.
- En el caso de que la información a enviar fuera de la entidad corresponda con datos personales catalogados como categorías especiales de datos, (como 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 así como los relativos a condenas e infracciones penales), el archivo se enviará cifrado (por ejemplo, comprimido con contraseña con el programa Winzip).
- Si se requieren datos personales por parte de juzgados, policía judicial o de las Fuerzas y Cuerpos de Seguridad del Estado, se les indicará que deben dirigirse al correo electrónico datos@caritas-sc.org. En ningún caso el personal les facilitará información, ni siquiera verbalmente.

# D. Incidencias de seguridad y solicitud de derechos

## 14. Coordinador de protección de datos.

Ante el coordinador de protección de datos, el empleado o voluntario deberán:

- 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

## 15. Incidencias y brechas de seguridad.

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. Son incidencias:

## 16. Solicitudes de derechos

Si una persona nos pide que eliminemos sus datos personales de nuestros ficheros o realiza cualquier otra petición relacionada con sus datos personales (cancelación, modificación, acceso...), el personal que recibe la solicitud la hará llegar de inmediato a los correos electrónicos indicados en la hoja de consentimiento y, en todo caso y especialmente, a datos@caritas-sc.org

Asimismo, se recuerda que el personal será responsable frente a la entidad y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a la entidad 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, voluntarios y colaboradores de la entidad, el trabajador, voluntario o colaborador declara que lo ha leído y comprendido en toda su extensión.

Firmado:

El trabajador/voluntario/alumno en prácticas/ colaborador _____
con DNI _____

En _____, a __ de _____ de 20__